Seguridad, Privacidad y Vigilancia

Antonio Carrillo Ledesma
Karla Ivonne González Rosas

Seguridad, Privacidad y Vigilancia

Antonio Carrillo Ledesma y Karla Ivonne González Rosas
Facultad de Ciencias, UNAM
http://academicos.fciencias.unam.mx/antoniocarrillo

La última versión de este trabajo se puede descargar de la página:
https://sites.google.com/ciencias.unam.mx/acl/en-desarrollo
http://132.248.181.216/acl/EnDesarrollo.html

2025, Versión 1.0α[1]

Índice

1 Introducción **5**
1.1 Computadoras Actuales 9
1.2 Sistemas Operativos 53
1.3 Seguridad TIC 55
1.4 Formación en Seguridad de la Información 58
1.5 ¿Qué tan Seguro es Linux/Unix? 60
1.6 Agradecimientos 64

2 Sistemas Operativos **66**
2.1 Windows 83
2.2 UNIX y BSD 90
2.3 Apple y sus macOS e iOS 92
2.4 GNU/Linux 97
2.5 Android 111
2.6 Chromebook y Chrome OS 114
2.7 Otros Sistemas Operativos 117

3 Seguridad, Privacidad y Vigilancia **124**
3.1 ¿Qué es la Privacidad y por qué es Importante? 125
3.2 Las Vulnerabilidades y Exposiciones Comunes 132
3.3 Alfabetismo Digital 134
3.4 Amenazas a la Ciberseguridad 136
3.5 Dicen que si no Pagas por un Producto, Entonces el Producto Eres Tú. 144
3.6 Datos que Recopila Google 147
3.7 ¿Cómo me Protejo? 150

4 Recomendaciones de Ciberseguridad **154**
4.1 Uso de Contraseñas Robustas 154
4.2 Mantener Actualizado el Sistema Operativo y Aplicaciones . . 159
4.3 Cifrar Dispositivos, Discos y Unidades de Respaldo 162
4.4 Generar Respaldos y Validar su Restauración 167
4.5 Navegación Segura 169
4.6 Mensajería Instantánea 178
4.7 Banca en Línea Segura 180
4.8 Uso Seguro de las Herramientas de la Nube 181

4.9 Protección de Teléfonos, Tabletas y Computadoras 182
4.10 Escaneo de Códigos QR de Forma Segura 186
4.11 Uso de Redes Sociales Responsablemente 189
4.12 Seguridad en Videoconferencias 194
4.13 Cómo Tomar, Enviar y Almacenar Contenido Íntimo 196
4.14 Protección Contra Ataques con Técnicas de Inteligencia Social 205
4.15 Protección de Dispositivos Personales en Redes Corporativas . 210
4.16 Uso de Escritorios Remotos y Virtuales 211
4.17 Máquinas Virtuales 213
4.18 Protegiendo Nuestros Metadatos 215
4.19 Averiguar Todo Sobre Cualquier Persona en Internet 219
4.20 Prácticas de Ciberseguridad para Viajeros 223

5 Meltdown, Spectre y lo que se Acumule 227
5.1 ¿Qué es Meltdown? 229
5.2 ¿Qué es Spectre? 230
5.3 Falla en los Procesadores Snapdragon 231
5.4 Falla en el Chip T2 de las Mac 232
5.5 Falla en el Chip M1 de las Mac 233
5.6 GhostRace 235
5.7 Caballo de Troya de Hardware 237

6 Distribuciones Seguras, Penetración, Inmutables y IOT 241
6.1 Distribuciones de GNU/Linux «Seguras» 243
6.2 Distribuciones de GNU/Linux «Para Penetración» 246
6.3 Distribuciones de GNU/Linux «Inmutables» 248
6.4 Distribuciones de GNU/Linux para el «Internet de las Cosas» 252
6.5 Otras Distribuciones Útiles 254

7 Tecnología para el Teletrabajo 256
7.1 VDI en el Teletrabajo: Ventajas e Inconvenientes 257
7.2 VPN en el Teletrabajo: Ventajas e Inconvenientes 259

8 Seguridad y Privacidad en el Software 261
8.1 Consideraciones de Seguridad 262
8.2 Consideraciones Sobre la Privacidad 270
8.3 Software Libre e Infraestructura Crítica 276

9 Búsquedas en Deep y Dark Web **283**
9.1 ¿Qué es Web Superficial, la Deep y Dark Web? 283
9.2 Acceso a la Deep Web 285
9.3 Acceso a la Dark Web 286
9.4 Tipos de Amenazas en la Web Oscura 291
9.5 Cómo Podemos Entrar en la Internet Oculta 295
9.6 ¿Cómo funciona TOR? 299

10 Internet y Puertos **304**
10.1 Escaneo de Puertos 306
10.2 Cortafuegos 314
10.3 Acceso Remoto Mediante SSH 320
10.4 Copiar Archivos Entre Equipos 326

11 Apéndice A: Software Libre y Propietario **332**
11.1 Software Propietario 335
11.2 Software Libre 337
11.3 Seguridad del Software 344
11.4 Tipos de Licencias 347
11.4.1 Licencias Creative Commons 353
11.4.2 Nuevas Licencias para Responder a Nuevas Necesidades 355
11.5 Implicaciones Económico-Políticas del Software Libre 358
11.5.1 Software Libre y la Piratería 358
11.5.2 ¿Cuánto Cuesta el Software Libre? 359
11.5.3 La Nube y el Código Abierto 362
11.5.4 El Código Abierto como Base de la Competitividad . . 365
11.5.5 Software Libre en Empresas y Corporaciones 366
11.6 Código Abierto y las Organizaciones Internacionales 374
11.6.1 Las Naciones Unidas y el Código Abierto 375
11.6.2 La Comisión Europea se Compromete a Liberar Todo el Software que Pueda Beneficiar a la Sociedad 376

12 Apéndice B: Máquinas Virtuales **379**
12.1 Tipos de Máquinas Virtuales 380
12.2 Técnicas de Virtualización 381
12.3 Otras Formas de Virtualización 382
12.4 Aplicaciones de las Máquinas Virtuales de Sistema 384
12.5 Ventajas y Desventajas 386

12.5.1 Ventajas 386
12.5.2 Desventajas 388
12.5.3 Consideraciones Técnicas y Legales de la Virtualización 389
12.6 Máquinas Virtuales en la Educación, Ciencias e Ingeniería . . 390
12.7 ¿Qué Necesito para Crear y Usar una Máquina Virtual? 393
12.8 ¿Cómo Funciona una Máquina Virtual? 395
12.9 Aplicaciones y Paquetes Disponibles 396
12.10 Acceso a Datos Desde una Máquina Virtual 402
12.11 Desde la Nube 403

13 Apéndice C: Escritorios Remotos y Virtuales 406
13.1 Escritorio Remoto 410
13.1.1 Escritorio Remoto de Chrome 410
13.1.2 Escritorio Remoto de Windows 413
13.2 Escritorio Virtual 415
13.2.1 Escritorios y Máquinas Virtuales con VNC 416
13.3 Desde la Nube 422

14 Bibliografía 425

1 Introducción

Las tecnologías de la información y comunicación (TIC) son el resultado de poner en interacción la informática y las telecomunicaciones. Todo, con el fin de mejorar el procesamiento, almacenamiento y transmisión de la información.

Consiguiendo de esta manera mejorar el nivel de nuestras comunicaciones. Creando nuevas formas de comunicación más rápida y de mayor calidad. Mejoras que reducen costes y tiempo, de aplicación tanto al mundo de la educación, los negocios como a la vida misma. Proporcionándonos una mayor comodidad y mejorando nuestra calidad de vida a la vez que se aboga por el medio ambiente.

No descubrimos nada si decimos que el impacto de internet en nuestra vida cotidiana aumentó y se aceleró con la pandemia. Sino basta con revisar las actividades que se convirtieron en rutina durante el confinamiento, como las clases a distancia, el teletrabajo, o actividades de entretenimiento, por mencionar algunas. Sin embargo, más allá de la infinidad de beneficios y oportunidades que representa internet, también tiene sus riesgos, y así como puede proporcionar satisfacciones que motivan el constante desarrollo de la tecnología, también puede ser la causa de varios dolores de cabeza. Por supuesto, todo depende de la forma en que se utiliza, ya que las consecuencias de su uso dependerá de las prácticas y el comportamiento de los usuarios.

En este sentido y considerando que internet representa un pilar clave en las sociedades actuales, es importante hablar de normas de convivencia y del rol y la responsabilidad que tienen los usuarios para lograr que sea, cada vez más, un ambiente agradable, respetuoso y seguro; algo que sin duda beneficiará a todos.

Sobre Amenazas y Vulnerabilidades informáticas Antes de entrar de lleno en las Amenazas y Vulnerabilidades informáticas, dejaremos en claro brevemente qué son las mismas, y en qué se diferencian ambas.

- Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros»

pueden tener distintos orígenes por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

- Por su parte, una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

Pequeñas acciones, grandes cambios el concepto de netiqueta es utilizado para referirse a un conjunto de reglas o pautas de comportamiento a la hora de utilizar e interactuar a través de algún servicio de internet, como pueden ser foros, Blogs, juegos en línea, redes sociales o el correo electrónico. En otras palabras, se trata de trasladar las normas de educación del ambiente físico al ámbito digital.

Cuando hablamos de buenas prácticas de convivencia como ciudadanos digitales no nos referimos solamente a los aspectos comunicacionales, sino también relacionados con la seguridad. Prácticas que pueden ayudar a evitar poner en riesgo a otros usuarios. Por ejemplo, cuando un usuario rompe una cadena con información falsa o un contenido que resulta ofensivo para otros usuarios.

Dicho esto, además de evitar compartir contenido inapropiado, es importante que los usuarios tengan presente que también pueden reportar a un usuario o contenido para que sea eliminado y de esta forma evitar que llegue a más usuarios. En un sentido amplio, los usuarios también podemos involucrarnos para generar mayor conciencia entre las personas que conocemos y estimamos.

Los resultados pueden ser diversos, pero lo que es un hecho es que al igual que en el plano físico, las acciones individuales, por más pequeñas que sean, cuentan y contribuyen a que internet sea un espacio en el que se promuevan más las actitudes positivas, valores, acciones responsables y en general, la cordialidad y respeto que nos gustaría recibir de parte de los otros.

Educación, buenas prácticas y tecnología de seguridad si bien respetar las normas de comportamiento en internet es fundamental para lo-

grar el propósito de generar un espacio más cordial, la seguridad en internet requiere de otros elementos, como la aplicación de buenas prácticas de seguridad en el uso de la tecnología, y por supuesto, de la educación de los usuarios, para de esta manera estar cada vez más y mejor informados.

En este sentido, advertir a tus contactos sobre algún engaño que está circulando, revisar la configuración de la privacidad y seguridad de tus cuentas, evitar compartir información de personal a desconocidos o información de terceros sin su autorización, así como compartir archivos sin antes verificar que sean seguros, son apenas algunas de las recomendaciones para que internet sea un espacio más seguro. Sobre todo en estos tiempos en los que pasamos más tiempo conectados y en el que la circulación de Fake News y engaños parecen ser moneda corriente.

En conjunto con lo anterior, no se debe dejar de lado el uso de las tecnologías de seguridad que en la actualidad resultan básicas debido a la cantidad, complejidad y diversidad de las amenazas informáticas que se propagan por internet. Estas acciones en conjunto nos permitirán utilizar la tecnología de una forma cada vez más consciente, responsable y, por supuesto, segura.

¿Qué componen las tecnologías de la información y comunicación? los dispositivos de cómputo, las redes y los servicios, por tanto, también pueden ser clasificadas según hagan un uso u otro de estos elementos. En relación a los dispositivos mucho es lo que se ha avanzado. La computadora personal ha evolucionado desde su aparición y sigue haciéndolo a un ritmo vertiginoso. Al igual que los aparatos periféricos que lo complementan, ofreciendo otras posibilidades.

La tecnología no se ha estancado en las computadoras personales. Nos va sorprendiendo introduciendo nuevos tipos de terminales en nuestras vidas o mejorando sus características. ¿Qué fue de aquel teléfono móvil cuya única función era llamar?. Ahora son dispositivos mucho más sofisticados que han revolucionado la comunicación. Las vídeo llamadas, las aplicaciones de mensajes de texto gratuitas, las redes sociales, etc. son algunos ejemplos.

En cuanto a las redes que permiten que los dispositivos estén interconectados, la piedra angular sería el internet. Su impacto en la sociedad no se puede explicar en unas líneas, pero es lo que hace girar este mundo. Las TICs han hecho un arduo trabajo en el campo de las redes. Mejorando la telefonía fija, la telefonía móvil, el propio internet pasando de la conexión telefónica a la banda ancha, después a la fibra óptica y llevando la conexión

a los móviles. Permitiendo así que estemos informados al momento.

El otro elemento que conforman las tecnologías de la información y la comunicación, son los servicios. Cada vez es más grande el abanico de servicios que se nos ofrece: correo electrónico, búsqueda de información, banca online, comercio electrónico, e-administración, e-gobierno, servicios privados, servicios de ocio, etc.

Ante el constante aumento -explosivo- en el uso de dispositivos como computadoras personales, Laptops, tabletas y teléfonos celulares, expertos en ciberseguridad advierten un entorno propicio para que prosperen los cibercriminales y que, tanto individuos como empresas, se encuentran mayormente expuestos a múltiples amenazas de ciberseguridad.

En la actualidad, aproximadamente la mitad de la población mundial accede de algún modo a internet. Con tantos accesos concurrentes a la red de redes, la posible amenaza de seguridad a los sistemas informáticos crece y se complejiza, a pesar de las diversas y especializadas maneras de contrarrestarlas. En la gran mayoría de los casos, el eslabón más débil de la ciberseguridad es el factor humano, que representa la vulnerabilidad más impredecible de cualquier sistema informático. Son las personas las que "caen" en una campaña de Phishing o Whaling, que usan el nombre de la mascota como contraseña. Estas personas son las primeras en abrir las puertas a los ciberdelincuentes.

Al estar cada vez más interconectados y, como resultado de esto, la exposición a las vulnerabilidades de seguridad también ha aumentado dramáticamente. Las complejidades de mantener las plataformas de cómputo actuales hacen que sea muy difícil para los desarrolladores cubrir cada punto de entrada potencial. En 2019 hubo un promedio de más de 45 vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures, CVE) registradas por día y estas siguen en aumento año con año. Los ataques de seguridad vienen en muchas formas y usan varios puntos de entrada. Cada tipo de ataque viene en varios tipos, ya que generalmente hay más de una forma en que se pueden configurar o camuflar en función de la experiencia, los recursos y la determinación del pirata informático.

Antes de iniciar con los tópicos de seguridad, Privacidad y Vigilancia, es necesario conocer cómo está constituida nuestra herramienta de trabajo: la computadora. Los conocimientos básicos de arquitectura de las computadoras nos permiten identificar los componentes de Hardware que juegan un papel preponderante en el rendimiento del equipo y prestarles la atención que requiere cuando se adquiere un equipo de cómputo.

1.1 Computadoras Actuales

La computadora (también conocida como ordenador) actual es una máquina digital programable que ejecuta una serie de comandos para procesar los datos de entrada, obteniendo convenientemente información que posteriormente se envía a las unidades de salida. Una computadora está formada físicamente por numerosos circuitos integrados y varios componentes de apoyo, extensión y accesorios, que en conjunto pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa (Software).

La constituyen dos partes esenciales, el Hardware, que es su estructura física (circuitos electrónicos, cables, gabinete, teclado, etc.), y el Software, que es su parte intangible (programas, datos, información, documentación, etc.).

Con respecto al Hardware[1], se encuentra compuesto por una serie de dispositivos, clasificados según la función que estos desempeñen. Dicha clasificación se compone de:

- Los dispositivos de entrada son todos aquellos que permiten la entrada de datos a una computadora. Estos dispositivos (periféricos), son los que permiten al usuario interactuar con la computadora. Ejemplos: teclado, Mouse (ratón), micrófono, Webcam, Scanner, etc.

- Los dispositivos de salida, son todos aquellos que permiten mostrar la información procesada por la computadora. Ejemplos: monitor, impresora, auriculares, altavoces, etc.

- Los dispositivos de comunicación son aquellos que permiten la comunicación entre dos o más computadoras. Ejemplos: Modem, Router, placa de red, Bluetooth, etc.

[1] En Debian GNU/Linux podemos instalar la aplicación *lshw* para conocer los distintos componentes de la computadora, mediante:

```
# apt install lshw
```

Así, para ver de forma resumida los dispositivos que componen la computadora usamos:

```
# lshw -short
```

Si necesitamos más detalle usamos:

```
# lshw
```

- Los dispositivos de almacenamiento, son todos aquellos que permiten almacenar datos en el ordenador. Ejemplos: disco duro, Pendrive, Diskette, CD y DVD, etc.

- Los dispositivos de cómputo, son aquellos encargados de realizar las operaciones de control necesarias, sobre el resto de los dispositivos la computadora.

La unidad central de procesamiento (Central Processing Unit CPU) se comunica a través de un conjunto de circuitos o conexiones llamada Bus de datos o canal de datos. El bus conecta la CPU a los dispositivos de almacenamiento, los dispositivos de entrada y los de salida.

En la actualidad, una computadora puede tener una CPU de 32 o de 64[2] bits para describir anchura de registros, Bus de direcciones, Bus de datos o instrucciones. Es decir que la cantidad de bits nos permite diferenciar el tipo de CPU que tiene nuestro equipo.

La CPU, el sistema operativo, el Software en general y los Drivers se basan en una misma arquitectura, pero que tenga más o menos bits puede ser significativo en la experiencia del usuario.

[2] ¿Por qué se llama x86 a la de 32 bits y x64 a la de 64 bits?

Por pereza. El término adecuado para la arquitectura de 64 bits basada en las tecnologías desarrolladas por Intel y AMD desde 1976 es x86-64, que es como la llamó AMD cuando la desarrolló.

El término "x86" se acuñó porque Intel denominó 8086 a la primera CPU que utilizaba esta microarquitectura. Era una CPU de 16 bits con un conjunto de instrucciones similar al anterior Intel 8085 de 8 bits, por lo que Intel le dio un número más alto. A principios de los años 90, a los desarrollos posteriores de la 8086 se les asignaron números que terminaban en "86": 80186, 80286, 80386 y 80486. En la mayoría de los casos, se omitió la parte "80" y toda la familia de CPU se denominó "x86", por razones obvias. Con lo que habría sido el 80586, Intel eliminó los números porque no podían registrarlos como marca, así que nació la marca "Pentium", que primero significaba quinta generación, pero luego como una simple marca.

Cuando Intel pasó a los 32 bits con el conjunto de instrucciones x86 con el 386 en 1985, no cambiaron la marca de nada, pero cuando AMD extendió x86 a 64 bits, lo comercializaron como x86-64. Muchos desarrolladores de Software lo llamaron "AMD64" en su lugar, ya que AMD lo desarrolló. Intel no estaba dispuesto a hacer eso, así que lo llamaron "EMT64" cuando adoptaron las extensiones de 64 bits de AMD después del fracaso de Itanium. Al final, la mayoría de la gente simplemente lo llamó "x64", aunque esto no tiene ningún sentido.

En la actualidad, la mayoría de ordenadores cuentan con CPU de 64[3] bits. Ahora bien, todavía hay equipos algo antiguos que cuentan con la arquitectura de 32 bits, por lo que sigue coexistiendo en el mercado y el sector hace desarrollos también pensando en sus capacidades.

Desde el punto de vista funcional es una máquina que posee, al menos, una unidad central de procesamiento, unidad de memoria (Random Access Memory RAM , Read Only Memory ROM y Caché) y dispositivos de entrada/salida (periféricos). Los periféricos de entrada permiten el ingreso de datos, la CPU se encarga de su procesamiento (operaciones aritmético-lógicas) y los dispositivos de salida los comunican a los medios externos. Es así, que la computadora recibe datos, los procesa y emite la información resultante, la que luego puede ser interpretada, almacenada, transmitida a otra máquina o dispositivo o sencillamente impresa; todo ello a criterio de un operador o usuario y bajo el control de un programa de computación.

[3] ¿Alguna empresa ha fabricado una CPU de 128 bits?

Si alguien quiere fabricar una CPU de 128 bits, puede utilizar el diseño RISC-V, que admite núcleos de 32, 64 y 128 bits. No hay problema, solo se necesita un diseño adecuado y listo. Muchos dicen que el beneficio de una CPU (núcleo) de 64 bits es la enorme memoria direccionable, 64 bits en comparación con los 32 bits de los núcleos de 32 bits. ¡Pero eso no es cierto!. Todos los núcleos de 64 bits (excepto los muy especiales) tienen un bus de direcciones de 52 o 56 bits. Windows y Linux utilizan internamente un espacio de direccionamiento de a lo más 48 bits. No hay necesidad de memoria física de 64 bits porque hoy en día no es posible tenerla (teóricamente hasta 16 Exabytes).

Algo similar ocurre con los núcleos de 128 bits. Como la memoria no es importante, lo único que queda es la matemática de 128 bits. La pregunta es: ¿quién necesita la matemática de 128 bits? En 1978, el 8086 tenía un coprocesador matemático, el 8087, que admitía tipos de punto flotante de 80 bits. Hoy en día, es similar, pero el tipo máximo admitido sigue siendo de 64 bits que tiene aproximadamente 16 dígitos decimales de precisión con un rango del orden de 1.7×10^{-308} a 1.7×10^{308}, el número de 32 bits que tiene 14 dígitos decimales de precisión con un rango del orden de 3.4×10^{-38} a 3.4×10^{38}. Además, existe el número de 80 bits que tiene 18 dígitos decimales de precisión con un rango del orden de 3.4×10^{-4096} a 1.1×10^{4096}.

En algunos compiladores existen 128 bits de datos, pero no existe matemática de Hardware, sino que se implementa en Software. Se necesitan tipos tan grandes en muy pocas circunstancias.

Lo que importa hoy en día es la paralelización, el procesamiento de múltiples tipos en paralelo. Durante mucho tiempo, x86 ha tenido AVX512, que es un motor matemático de 512 bits (reemplazó al 8087), pero es capaz de trabajar con tipos de 8 a 64 bits en paralelo, por ejemplo, 8 operaciones matemáticas en paralelo utilizando FP64 (punto flotante de 64 bits).

CPU la Unidad Central de Proceso (Central Processing Unit CPU) es aquella parte del procesador que se encarga de ejecutar las diversas acciones que ordenemos al dispositivo que debe llevar a cabo. La CPU es el componente básico dentro de todo dispositivo inteligente, ya que prácticamente cualquier proceso que se ordene al sistema pasa por él. Con el paso del tiempo, además, su eficiencia y calidad ha alcanzado grandes cotas, aunque tecnologías al alza como las NPU han supuesto un mayor salto cualitativo que el de aumentar la potencia bruta de la CPU.

GPU, para el procesamiento gráfico la Unidad de Procesamiento Gráfico (Graphics Processing Unit GPU) es el apartado que se dedica a las acciones de mayor peso: las de componente gráfico. De este modo, acciones como la ejecución de videojuegos, o la edición y renderizado de vídeos, se llevan a cabo a través de la GPU del sistema. La calidad del teléfono, ordenador u otro dispositivo inteligente, suele ir supeditada a menudo a la calidad de su GPU, que dependerá de la banda de precio del aparato en cuestión. Eso sí, si los otros componentes no tienen la misma calidad, se puede producir el temido cuello de botella.

En los smartphones, la GPU ya va integrada en los procesadores, pero en los PC's, como AMD y NVIDIA se muestran como marcas especializadas en las GPUs. Cuentan con todo tipo de gamas y también poseen un amplio abanico de precios, un valor siempre directamente proporcional a la calidad y capacidad de sus gráficas, y a su vigencia en el mercado.

NPU, redes neuronales en tu dispositivo la Unidad de Procesamiento Neuronal (Neural Processing Unit NPU), a diferencia de la GPU, que cuenta con un funcionamiento paralelo al de la CPU, puede encargarse de funciones similares a las de la CPU, pero lo hace de un modo mucho más eficiente. Impulsada por Inteligencia Artificial, una NPU[4] es capaz de priorizar procesos para ejecutarlos de un modo exponencialmente más veloz y con un consumo mucho menor. En móviles, se usa especialmente para mejorar el procesado de fotografías, aunque participa en muchos otros procesos.

Además, esta arquitectura todavía tiene años de progreso por delante, a

[4]Para muestra, la compañía Cerebras con su procesador WSE-3 aglutina 4 billones de transistores, tiene una superficie de 46,225 mm^2, integra nada menos que 900,000 núcleos optimizados para IA y es capaz de entrenar hasta 24,000 millones de parámetros, lo que también equivaldría a un rendimiento máximo de IA de 125 petaflops.

diferencia de la CPU y la GPU, cuyas mejoras ya son de carácter más leve y basadas en aumentar la potencia bruta. La tecnología NPU, en cambio, lleva menos tiempo entre nosotros y todavía tiene mucho margen de mejora para ofrecer un rendimiento cada vez más poderoso.

Desde la llegada de los procesadores de más de un núcleo a PC, como consecuencia de la imposibilidad de hacerlos escalar en potencia solo por velocidad de reloj, la forma de entender los diferentes chips cambió. Han pasado ya dos décadas de dicho cambio y ante la inminente salida de los Chips disgregados o por Chiplets al mercado de masas, no está de más recordar la organización más común en el mundo del Hardware en todo este tiempo.

¿Qué es un SoC? las siglas SoC significan System on a Chip y hace referencia a todo chip que tiene la mayoría de componentes integrados en una misma pieza de silicio sin llegar a ser un microcontrolador. Se trata de la pieza de Hardware más usada por el hecho de que a día de hoy todo procesador para PC, teléfono móvil, consola de videojuegos, televisor o incluso servidores, es un SoC y pese a las diferencias entre ellos, todos tienen una organización común.

En realidad, todas las CPU actuales son SoC, ya que se trata de "varias CPU" diseñadas para funcionar alrededor de un elemento de intercomunicación central. Este se encarga de interconectar los diferentes elementos entre sí y de darles acceso a interfaces externas.

Por ejemplo, con la memoria RAM (u otros), a la que está asociado el controlador de memoria que comparten todos sus elementos o a los periféricos, y a los cuales se puede acceder directamente con una serie de interfaces específicas, o a través de un Chipset externo encargado de gestionar los diferentes periféricos y componentes.

En PC, debido a que la comunicación con los periféricos se hace a través del uso de direcciones de memoria de la RAM principal, los componentes relacionados con esta se encuentran subordinados al controlador de memoria. Por lo que son una pieza más conectada a la parte central.

¿Qué es una APU y en qué se diferencia de un SoC? las siglas APU significan Accelerated Processor Unit y fue usada por AMD cuando sus CPU e iGPU (o GPU integrada, la veremos a continuación) no traían consigo ningún sistema de gestión de E/S (entrada y salida). Sin embargo, la cosa empezó a cambiar ya con la arquitectura "Carrizo" que fue el nombre

clave de los últimos SoC antes del lanzamiento de los AMD Ryzen, donde se incorporaron varias interfaces de periféricos directamente en la CPU.

A día de hoy todo es un SoC, lo que ocurre es que, en sobremesa, las torres tienen tanta conectividad y capacidad de expansión que se suele emplear un Chipset, y lo mismo ocurre en estaciones de trabajo y servidores, pero no en el resto. Y es que si hablamos de un Chip para un PC portátil, una consola o un móvil, entonces al no existir tantas interfaces para periféricos y otros componentes, entonces estás se pueden integrar en un mismo chip.

En realidad, el término APU es más bien comercial de AMD y al día de hoy se utiliza como sinónimo de SoC, pero se puede resumir en que una APU carece de cualquier gestión de periféricos y requiere de un Chip externo para ello. Mientras que un SoC tiene las especificaciones mínimas en ese aspecto, pese a ser también ampliables. Para simplificar la idea, un SoC es una APU más completa.

¿¡GPU qué es y cuáles son sus características concretas frente a una dGPU? las siglas iGPU corresponden a integrated GPU, y hace referencia a todo componente de este tipo que se encuentre integrado en una APU o un SoC. Por lo que se trata de procesadores gráficos de potencia limitada que se pueden ver lastrados en velocidad de reloj por el problema del ahogamiento termal (Thermal Throttling) que se produce cuando muchas partes comparten el mismo espacio físico.

Si bien, es posible llegar a ciertos niveles de rendimiento que son aceptables de cara a reproducir las escenas en 3D a tiempo real en los videojuegos, y otras tareas de carácter profesional donde se usa una tarjeta gráfica, estas se ven cuanto menos limitadas:

El hecho de tener que compartir espacio en el mismo Chip con los diferentes núcleos de la CPU produce que esta no pueda alcanzar la misma velocidad de reloj que se alcanzaría siendo un Chip aparte e independiente.

En PC, debido a que como la memoria RAM usa DDR o LPDDR, el ancho de banda es pequeño y hemos de partir del hecho de que el rendimiento de todo Chip gráfico, incluido una iGPU, depende del ancho de banda que se le puede otorgar con dicha memoria RAM.

Los SoC con iGPU actuales tienen un tamaño fijo, definido este por la cantidad de pines soportados por la interfaz con la placa base. Esto limita el tamaño, no solo del Chip, sino también de la gráfica integrada en el mismo.

iGPU en consolas de videojuegos al contrario de lo que ocurre con los PC, las consolas de videojuegos no tienen que seguir una serie de normas respecto a sus componentes. Para empezar, no ven el tamaño de sus chips limitados por un estándar de placa base, dado que son productos únicos y exclusivos. Esto les permite tener el tamaño que quieran, incluso más que una CPU convencional para PC, lo que les permite tener una iGPU en su SoC mucho más avanzada.

El otro punto es la memoria utilizada, ya que la de las tarjetas gráficas también se usan como memoria principal. Esta da el ancho de banda necesario para que la iGPU alcance cierto nivel de rendimiento, pero su latencia es mucho más alta que la RAM convencional de PC que está más optimizada en ese aspecto, por lo que el rendimiento de su CPU suele ser más bajo que su equivalente para ordenador.

¿Qué es una dGPU en un PC o portátil? las dGPU, o GPU dedicadas, no son otra cosa que las GPU de toda la vida, pero la particularidad es que también son SoC, ya que tiene varios núcleos, especializados en tareas gráficas, alrededor de una interfaz central y compartiendo todos ellos un mismo acceso a memoria.

Sin embargo, carecen de núcleos de CPU en su interior, de ahí a que no se les llame APU o SoC, por el hecho de que de existir estos elementos pasarían a ser una iGPU. Por lo tanto, su principal particularidad de las dGPU es que tienen su propia memoria RAM (SDRAM para ser concretos) la cual suele rodear estos Chips, ya sea en forma de tarjeta gráfica o soldados en la placa de los ordenadores portátiles. A esta la llamamos VRAM y es de uso exclusivo de la dGPU o GPU.

Los equipos de cómputo los podemos clasificar[5] por:

- Equipos móviles: estos equipos buscan un equilibrio entre su capacidad de cómputo versus el rendimiento energético de sus baterías -para operar el mayor tiempo posible sin recargarse- y su peso, entre estos equipos destacan las Laptops, Notebook, Netbook, Ultrabook, tabletas, teléfonos inteligentes, etc.

[5]El ordenador del Apollo 11, el Block II, funcionaba a una velocidad de 2 MHz y tenía 2 KB de memoria RAM y 32 KB de memoria ROM. Para ponerlo en contexto, el chip de un cargador USB-C moderno es 563 veces más potente que la computadora que se usó en el Apollo 11, al menos en términos de potencia bruta.

- Equipos de escritorio: estos equipos al estar permanentemente conectados a la corriente eléctrica pueden tener un mayor número de componentes y disponen de una mejor capacidad disipación de calor por lo que pueden contener una mayor cantidad componentes, como discos, RAM o tarjetas de video y el tamaño, peso o consumo energético no es un inconveniente.

- Servidores: son equipos que suelen atender a múltiples usuarios simultáneamente y disponen de gran cantidad de Cores, RAM, disco y son interconectados por red de alta velocidad con otros servidores para atender las crecientes necesidades de los centros de datos los cuales deben estar permanentemente en operación. Generalmente los equipos son montados en Racks con otras decenas de equipos, por lo que su arquitectura se ve limitada a una moderada generación de calor por parte de sus componentes ya que su sistema de ventilación es por aire para todo el Rack.

- Estaciones de trabajo: son equipos individuales diseñados para atender cargas computacionales intensas, por lo que requieren Hardware más complejo y potente como puede ser múltiples tarjetas de video (con decenas de miles de Cores gráficos) , discos (con cientos de Terabytes), gran cantidad de RAM (pueden llegar a superar el Terabyte) y sistema de refrigeración por aire o líquido, etc.

- Cómputo intensivo: son equipos interconectados por red de alta velocidad con procesadores y tarjetas gráficas dedicadas para el cálculo numérico que soportan cargas intensas por largos periodos de tiempo, los más comunes son los que forman parte de los Cluster que llegan a tener millones de cores.

FLOPS Una medida relativamente objetiva para analizar el rendimiento de un dispositivo suele ser medir sus operaciones de punto flotante por segundo o más conocidas como FLOPS[6]. Hay que tener en cuenta que la medición de FLOPS es muy compleja porque las diferentes operaciones en punto flotante

[6] El Cray-1 fue puesto marcha en 1975 y utilizaba una CPU a 80 MHz y llevaba integrada una unidad SIMD de 64 bits de precisión de punto flotante, lo cual fue un salto de gigante que permitió un salto de los 3 MFLOPS de potencia del CDC 6600 a los 160 MFLOPS en el Cray-1.

llevan diferentes cantidades de tiempo para ejecutarse. Y no todo el mundo utiliza las mismas operaciones para establecer los cálculos.

Por ejemplo, una división simple como 1/5, toma significativamente menos tiempo que el cálculo del logaritmo de 5. Por eso, se estableció el algoritmo de Linpack como un estándar representativo con el que poder medir todos los sistemas bajo el mismo baremo de FLOPS-.

Es importante señalar que el algoritmo de Linpack utiliza el formato en punto flotante de doble precisión (64 bits[7] que tiene aproximadamente 16 dígitos decimales de precisión con un rango del orden de 1.7×10^{-308} a 1.7×10^{308}). Sin embargo, como veremos la mayoría de los valores que dan los fabricantes son con precisión simple (32 bits que tiene 14 dígitos decimales de precisión con un rango del orden de 3.4×10^{-38} a 3.4×10^{38}). Además, los valores que dan los fabricantes suelen ser teóricos y en la práctica suelen ser inferiores debido a otros factores limitantes como la frecuencia de reloj o la velocidad de las memorias ROM y RAM.

Por tanto, aunque todos hemos acabado midiendo el rendimiento en FLOPS, no es una medida absoluta de la potencia del CPU ni de una GPU. Por ejemplo para algunos dispositivos tenemos:

Móviles El SoC Snapdragon 821 que monta una GPU Adreno 530 tiene una potencia de 519.2 gigaFLOPS (0.52 TFLOPS), y los Chips Apple A9X del iPad Pro alcanzan los 345.6 gigaFLOPS (0.35 TFLOPS), todos ellos

[7] ¿Por qué no hay un procesador de 128 bits, si los hay de 64 y 32 bits?

En gran medida, esto se reduce a la cuestión de qué se entiende realmente por "procesador de 64 bits". Al inicio de las computadoras electrónicas, un "procesador de 8 bits" tenía registros de 8 bits, pero la mayoría tenía direccionamiento de 16 bits (y la Unidad de Aritmética y Lógica ALU a veces tenía 4 bits, por lo que cuando se añadían dos registros de 8 bits, la CPU a menudo lo hacía en dos pasos, añadiendo los 4 bits inferiores y luego añadiendo por separado los 4 bits superiores más el acarreo de los 4 inferiores).

Hoy en día, hemos invertido un poco esa situación: un procesador de "64 bits" (más o menos) tiene direccionamiento de 64 bits, pero tiene registros de 128 bits, 256 bits y, en algunos casos, incluso de 512 bits. Pero como los usos de números mayores a 64 bits son bastante raros, esos registros más grandes se usan normalmente para realizar operaciones en una cantidad de operandos más pequeños con una sola instrucción. Por lo tanto, en lugar de una ALU que tiene la mitad del tamaño de un registro y realiza una sola operación en múltiples ciclos de reloj, tenemos una ALU que tiene entre 2 y 4 veces el tamaño de un registro normal y realiza múltiples operaciones en un solo ciclo de reloj.

Dependiendo de cómo prefieras ver las cosas, podrías argumentar razonablemente que una CPU actual de "64 bits" es en realidad una CPU de 128 bits, 256 bits o incluso 512 bits.

medidos con precisión simple de 32-bits.

CPU

- Intel Xeon W-3245: 1.4 TFLOPS
- Intel Core i9-9900X: 1.2 TFLOPS
- AMD Ryzen 9 3950X: 1.1 TFLOPS

Los procesadores de gama media-alta rondan el medio TFLOPS:

- AMD Ryzen 7 3700X: 546.0 GFLOPS - 0.55 TFLOPS
- Intel Core i9-9900: 499.0 GFLOPS - 0.50 TFLOPS
- AMD Ryzen 5 3600X: 461.0 GFLOPS - 0.46 TFLOPS

Tarjetas Gráficas Ojo: La tabla está ordenada por los valores en precisión simple (32-bit) primer columna

GPU	FP32 TFLOPS	FP64 TFLOPS
TITAN V	13.8	6.9
Radeon RX Vega 64	12.7	0.8
GeForce GTX 1080 Ti	11.3	0.4
GeForce GTX 1080	8.9	0.3
Radeon R9 Fury X	8.6	0.5
Radeon HD 7990	7.8	1.9
GeForce GTX 1070	6.5	0.2
Radeon RX 480	5.8	0.4
GeForce GTX 690	5.6	0.2
Radeon R9 290X	5.6	0.7
GeForce GTX 780 Ti	5.3	0.2
Radeon HD 6990	5.1	1.3
GeForce GTX 980	4.9	0.15
Radeon RX 470	4.9	0.3
Radeon R9 290	4.8	0.6
GeForce GTX Titan	4.7	1.5
GeForce GTX 1060	4.4	0.14
Radeon HD 7970 GHz	4.3	1.1
GeForce GTX 780	4.1	0.17

Radeon R9 280X	4.0	1.0
Radeon R9 280	3.3	0.83
GeForce GTX 680	3.1	0.13
Radeon HD 7950	2.9	0.71

Como podemos ver, las tarjetas gráficas de Nvidia, normalmente, tienen una potencia muy alta en precisión simple, pero muy mala en precisión doble. La precisión simple es la que se usa en los juegos, pero la precisión doble es la que se utiliza en los cálculos complejos científicos y en el minado de muchas criptomonedas.

Consolas Todas ellos son en valores de precisión simple (32-bit)

- PlayStation 4: 1.3 TFLOPS
- Xbox One: 1.8 TFLOPS
- PlayStation 4 Pro: 4.2 TFLOPS
- Nintendo Switch: entre 0.4 y 0.5 TFLOPS
- PlayStation 5 promete una GPU con 10.28 TFLOPS
- La Xbox Series X promete una GPU de 12 TFLOPS

SuperCómputo Hace pocos se publicó la 64^a edición del ranking «Top 500» (noviembre del 2024) que clasifica los Clusters con mayor rendimiento del mundo. Esta lista se basa en la medida del rendimiento de los sistemas utilizando la prueba de referencia LINPACK, que calcula la velocidad a la que un sistema puede resolver un conjunto de ecuaciones lineales.

Y en esta nueva edición, los Clusters que ocuparon los primeros tres lugares son:

- El sistema El Capitan del Laboratorio Nacional Lawrence Livermore, en California, EE.UU., es el nuevo sistema número 1 del TOP500. El sistema HPE Cray EX255a ha obtenido 1.742 exaflop/s en el benchmark HPL. El Capitan tiene 11,039,616 núcleos y está basado en procesadores AMD EPYC(TM) de 4^a generación con 24 núcleos a 1.8 GHz y aceleradores AMD Instinct(TM) MI300A. Utiliza la red Cray Slingshot 11 para la transferencia de datos y alcanza una eficiencia energética de 60.3 Gigaflops/vatio.

- Frontier es ahora el sistema número 2 del TOP500. Este sistema HPE Cray EX fue el primer sistema estadounidense con un rendimiento superior a un exaflop/s. Está instalado en el Laboratorio Nacional Oak Ridge (ORNL) en Tennessee, EE.UU., donde se utiliza para el Departamento de Energía (DOE). Actualmente ha alcanzado 1.353 Exaflop/s utilizando 8,699,904 núcleos. La arquitectura HPE Cray EX combina CPUs AMD EPYC(TM) de tercera generación optimizadas para HPC e IA, con aceleradores AMD Instinct(TM) 250X y una interconexión Slingshot-11.

- Aurora es actualmente el número3 con una puntuación HPL preliminar de 1.012 Exaflop/s. Está instalado en Argonne Leadership Computing Facility, Illinois, EE. UU., donde también se opera para el Departamento de Energía (DOE). Este nuevo sistema de Intel se basa en HPE Cray EX - Intel Exascale Compute Blades. Utiliza procesadores Intel Xeon CPU Max Series, aceleradores Intel Data Center GPU Max Series y una interconexión Slingshot-11.

Para poner en contexto los avances en este campo, en el año 2004 IBM era dueña y señora del mundo de la supercomputación, su espectacular BlueGene/L dominaba la lista TOP 500. Aquel monstruo contaba con 32,768 procesadores PowerPC 440 a 700 MHz y 16 TB de memoria. 20 años después una sola NVIDIA GeForce RTX 4090 con 24 GB de memoria GDDR6X es más potente que esa supercomputadora -lo es al menos en rendimiento bruto-, BlueGene/L contaba en ese momento con un rendimiento de 70.72 TFLOPS, pero la propia NVIDIA dejaba claro en el lanzamiento de sus RTX 4090 que estas tarjetas gráficas contaban con una potencia de 83 TFLOPS.

Es más, cuatro RTX 4090 con soporte FP8 logran también rivalizar con la supercomputadora más potente de 2009. Y eso sin apretarle las tuercas a las RTX 4090: en noviembre de 2022 es precisamente lo que hicieron en Wccftech y lograron que la RTX 4090 se convirtiera en la primera tarjeta gráfica del mundo en alcanzar los 100 TFLOPS.

Esa comparación es como decimos real en esa potencia de cálculo en bruto, pero también es cierto que en esa y otras supercomputadoras se tenian mecanismos especiales de comunicación entre procesadores o de transferencia de datos, algo para lo que las GPUs actuales, aún siendo sobresalientes, no están tan optimizadas.

¿Cómo Trabaja una Computadora? Todas las computadoras sean de uno o más procesadores ejecutan los programas realizando los siguientes pasos:

1. Se lee una instrucción
2. Se decodifica la instrucción
3. Se encuentra cualquier dato asociado que sea necesario para procesar la instrucción
4. Se procesa la instrucción
5. Se escriben los resultados

Esta serie de pasos, simple en apariencia, se complican debido a la jerarquía de memoria RAM, en la que se incluye la memoria Caché, la memoria principal y el almacenamiento no volátil como pueden ser los discos duros o de estado sólido (donde se almacenan las instrucciones y los datos del programa), que son más lentos que el procesador en sí mismo. Con mucha frecuencia, el paso (3) origina un retardo muy largo (en términos de ciclos del procesador) mientras los datos llegan en el bus de la computadora.

Durante muchos años, una de las metas principales del diseño microinformático ha sido la de ejecutar el mayor número posible de instrucciones en paralelo, aumentando así la velocidad efectiva de ejecución de un programa. No obstante, estas técnicas han podido implementarse en Chips semiconductores cada vez más pequeños a medida que la fabricación de estos fue progresando y avanzando, lo que ha abaratado notablemente su costo.

El procesador es el cerebro de un ordenador. No hay que olvidar otros componentes como la memoria, el almacenamiento o la tarjeta gráfica dedicada, desde luego, pero el procesador está un escalafón por encima en la jerarquía.

Piensa que, si cambiamos el procesador en dos equipos con la misma memoria, almacenamiento o tarjeta gráfica, el comportamiento puede variar notablemente. Sin embargo, para un mismo procesador, los cambios en el resto de componentes no impactan de forma tan directa en la experiencia de uso de un equipo.

¿Qué es una CPU? Antes de nada, vamos a definir exactamente lo que es una CPU o un procesador. Como bien indican sus siglas en inglés (Central Processing Unit) es la unidad de procesamiento -puede ser Intel, AMD, ARM, etc- encargada de interpretar las instrucciones de un Hardware haciendo uso de distintas operaciones aritméticas y matemáticas. Características principales de un procesador:

- Frecuencia de reloj. Este primer término hace referencia a la velocidad de reloj que hay dentro del propio procesador. Es un valor que se mide en Mhz o Ghz y es básicamente la cantidad de potencia que alberga la CPU. La mayoría de ellas cuentan con una frecuencia base -para tareas básicas- y otra turbo que se utiliza para procesos más exigentes -con un aumento en el consumo de energía y por ende un aumento en la temperatura del procesador, requiriendo sistemas de disipación de calor eficientes-.

- Consumo energético. Es normal que nos encontremos con CPU 's donde su consumo energético varía notablemente. Es un valor que se muestra en vatios (W) y como es obvio, aquellos procesadores de gama superior, serán más propensos a consumir más energía. Ante esto, es importante contar con un eficiente sistema de enfriamiento además de contar con una fuente de alimentación acorde a la potencia requerida por el procesador, la tarjeta gráfica y sus respectivos sistemas de enfriamiento.

- Número de núcleos. Con el avance de la tecnología, ya es posible encontrar tanto procesadores de Intel como de AMD que cuentan ya con decenas de núcleos. Estos cores son los encargados de llevar a cabo multitud de tareas de manera simultánea.

- Número de hilos. Si un procesador tiene Hyperthreading en el caso de Intel o SMT (Simultaneous Multi-Threading) en el caso de AMD, significa que cada uno de los núcleos es capaz de realizar dos tareas de manera simultánea, lo que se conoce como hilos de proceso. Por lo tanto, un procesador de cuatro núcleos físicos con Hyperthreading tendría ocho hilos de proceso, y sería capaz de ejecutar ocho órdenes al mismo tiempo -los hilos no tienen las mismas capacidades de un core real y en muchos casos su uso merma el rendimiento del CPU, pero los sistemas operativos los reconocen como si fueran cores reales-[8].

[8] El AMD EPYC 9845 de 160 núcleos y 320 hilos a una frecuencia de 2,00 GHz basada

- Memoria Caché. A la hora de "recordar" cualquier tarea, el propio ordenador hace uso de la memoria RAM. Sin embargo no es eficiente este proceso y por tanto es necesario que utilice la memoria Caché de la CPU para paliar esta deficiencia. El Caché se caracteriza porque se llega a ella de forma más rápida y puede ser tipo L1, L2 y L3.

- Zócalo. Es el tipo de conector con pines o Socket al que se conecta la placa base. Por ejemplo, las últimas de Intel suelen tener el Socket LGA 1200, mientras que las de AMD con Ryzen son AM4.

- Red. Si bien la red es un recurso indispensable en un equipo de cómputo, en el caso de equipos paralelos la velocidad de la red es el mayor cuello de botella en cuanto a rendimiento, por ello es necesario usar redes de alto desempeño como las de InfiniBand con un alto costo económico pero de alto desempeño que pueden llegar al orden de cientos de Gigabytes por segundo.

Nuevos Procesadores la creciente demanda de dispositivos de cómputo ha generado una gran variedad de procesadores, los podemos clasificar como:

- Procesador compuesto por múltiples núcleos de alta eficiencia -con un consumo energético reducido- que sacrifican potencia de procesamiento en aras de extender la carga útil de las baterías de los dispositivos móviles.

- Procesador compuesto por múltiples núcleos de alto rendimiento que pueden estar al tope de su capacidad sin generar excesivo calor y son especialmente usados en servidores y en cómputo intensivo.

- Procesadores compuestos por múltiples núcleos de alto rendimiento que pueden ajustar su velocidad de reloj de manera dinámica para tratar cargas de trabajo pesadas por un cierto tiempo -pues generan gran cantidad de calor-, por lo que requieren un sistema eficiente de enfriamiento, son ideales para estaciones de trabajo.

- Procesadores compuestos por múltiples núcleos híbridos que en lugar de tener un único tipo de núcleo multipropósito, estos Chips cuentan con dos grupos de núcleos. El primero de ellos, compuesto por

en Zen 5c, este se acompaña de 640 MB de caché L3.

múltiples núcleos de alta eficiencia, se encarga de procesar las tareas más livianas o en segundo plano que deba realizar un procesador, todo ello, con un consumo energético menor. El otro grupo, compuesto por múltiples núcleos de alto rendimiento, sigue una dinámica opuesta, su consumo ener-gético es superior, pero únicamente entran en funcionamiento cuando la tarea en cuestión requiere un extra de procesamiento.

Para gestionar esta división de núcleos híbridos, se ha integrado un "Thread Director", un elemento que se encarga de determinar qué núcleo procesa cada tarea. Las compañías, además, ha modificado cómo funciona la caché de sus procesadores:

- Cada núcleo de rendimiento tiene su propia caché L2.
- Cada cluster de núcleos de eficiencia tiene una "piscina" de memoria L2 común, de la que beben todos los núcleos que sean partícipes.
- Tanto los núcleos de rendimiento como los de eficiencia tienen acceso a una "piscina" de memoria L3 común para todos ellos.

Otros de los cambios que impactarán en el desempeño de las CPUs es el aumento de velocidad y una mayor cantidad de memoria Caché, compatibilidad con memorias DDR6 y con la interfaz PCIe 6.0.

Si los chips de CPU tienen miles de millones de transistores, ¿qué sucede si algunos se estropean? ¡Esto es muy común! La forma en que funciona la fabricación de CPU se llama "Binning". Por ejemplo, Intel siempre intenta fabricar i7, sin embargo, a veces ocurre algo durante la fabricación y no puede cumplir con el rendimiento anunciado. Por ejemplo, tal vez uno de los núcleos esté defectuoso y no pueda realizar el Hyper Threading que se necesita para un i7, por lo que básicamente degradan el i7 a un i5 que no necesita el Hyper Threading. Por lo tanto, eliminan el Hyper Threading para todos los núcleos (no solo para el defectuoso), reducen la frecuencia, desactivan parte de la memoria caché, etc. hasta que convierten el i7 defectuoso en un i5 completamente funcional. Luego, los i7 con peores defectos terminarán siendo i3 o Pentium o Celeron, según los defectos. De esta manera, se trata de no desperdiciar ni una sola CPU aunque sea defectuosa, porque un i7 defectuoso, a menos que sea extremadamente defectuoso, aún puede funcionar como un i5, i3, Pentium o Celeron.

PCIe PCI Express (Peripheral Component Interconnect Express), abreviado como PCIe, es una tecnología de conexión de Hardware utilizada para la comunicación de alta velocidad entre diferentes componentes de un equipo informático. Este estándar se ha convertido en la interfaz más habitual para la conexión de tarjetas de expansión, como tarjetas gráficas que sirven para correr juegos, tarjetas de sonido, tarjetas de red y dispositivos de almacenamiento de alta velocidad.

Una de las ventajas destacadas de PCI Express es su arquitectura de canales independientes, que permiten la transferencia simultánea de datos en ambos sentidos. Cada carril tiene una tasa de transferencia específica, medida en gigabits por segundo (Gbps), y la capacidad de un slot PCIe se expresa como el número de carriles que tiene. Esto se traduce en un ancho de banda total mayor, lo que facilita la conexión de dispositivos que requieren altas tasas de transferencia, como las tarjetas gráficas modernas o los dispositivos de almacenamiento de última generación.

Los diferentes tipos de ranuras de PCI Express según su tamaño PCIe X1 carriles 1, pines 18, PCIe x4 carriles 4, pines 32, PCIe x8 carriles 8, pines 49, PCIe x16 Carriles 16, pines 82.

Adicionalmente, también es interesante fijarse en las diferentes versiones que se han ido lanzando desde que PCIe se lanzó al mercado:

- PCIe 1.0 ancho banda 8 GB/s, velocidad de transferencia 2.5 GT/s
- PCIe 2.0 ancho banda 16 GB/s, velocidad de transferencia 5 GT/s
- PCIe 3.0 ancho banda 32 GB/s, velocidad de transferencia 8 GT/s
- PCIe 4.0 ancho banda 64 GB/s, velocidad de transferencia 16 GT/s
- PCIe 5.0 ancho banda 128 GB/s, velocidad de transferencia 32 GT/s
- PCIe 6.0 ancho banda 256 GB/s, velocidad de transferencia 64 GT/s

Características Arquitectónicas los procesadores Intel x86 admiten un formato de precisión extendido de 80 bits con un significado de 64 bits, que es compatible con el especificado en el estándar IEEE. Cuando un compilador usa este formato con registros de 80 bits para acumular sumas y productos internos, está trabajando efectivamente con un redondeo unitario de 2^{-64} en vez de 2^{-53} para precisión doble, dando límites de error más pequeños en un factor de hasta $2^{11} = 2048$.

Algunos procesadores Intel y AMD tienen una operación fusionada de multiplicación y suma (FMA), que calcula una multiplicación y una suma combinadas $x + yz$ con un error de redondeo en lugar de dos. Esto da como resultado una reducción en los límites de error por un factor 2.

Las operaciones FMA de bloques de precisión mixta $D = C + AB$, con matrices A, B, C y D de tamaño fijo, están disponibles en las unidades de procesamiento tensorial de Google, las GPU NVIDIA y en la arquitectura ARMv8-A. Para entradas de precisión media, estos dispositivos pueden producir resultados de calidad de precisión simple, lo que puede proporcionar un aumento significativo en la precisión cuando los bloques FMA se encadenan para formar un producto matricial de dimensión arbitraria.

Meltdown y Spectre El tres de enero del 2018 se dio a conocer al público, que 6 meses antes se habían detectado dos distintos fallos en los procesadores de los equipos de cómputo, comunicaciones y redes de internet que usamos. Esto para dar tiempo a los desarrolladores de procesadores y de sistemas operativos de implementar estrategias para mitigar el problema. Estos son problemas de diseño de los procesadores de Intel, AMD, IBM POWER y ARM, esto significa que procesos con privilegios bajos -aquellos que lanzan las aplicaciones de usuarios convencionales- podían acceder a la memoria del Kernel del sistema operativo[9].

Un ataque que explota dicho problema permitiría a un Software malicioso espiar lo que están haciendo otros procesos y también espiar los datos que están en esa memoria en el equipo de cómputo (o dispositivo móvil) atacado. En máquinas y servidores multiusuario, un proceso en una máquina virtual podría indagar en los datos de los procesos de otros procesos en ese servidor compartido.

Ese primer problema, es en realidad solo parte del desastre. Los datos actuales provienen especialmente de un grupo de investigadores de seguridad formados por expertos del llamado Project Zero[10] de Google. Ellos han publicado los detalles de dos ataques (no son los únicos[11]) basados en estos

[9] En GNU/Linux, el Kernel (si usamos una versión actualizada) nos indica las fallas del procesador a las que es vulnerable, usando:

```
$ cat /proc/cpuinfo
$ lscpu
```

[10] https://googleprojectzero.blogspot.com/

[11] Entre las distintas vulnerabilidades detectadas y sus variantes resaltan: Meltdown

fallos de diseño. Los nombres de esos ataques son Meltdown y Spectre. Y en un sitio Web dedicado a describir estas vulnerabilidades destacan que "aunque los programas normalmente no tienen permiso para leer datos de otros programas, un programa malicioso podría explotar Meltdown, Spectre y apropiarse de secretos almacenados en la memoria de otros programas". Como revelan en su estudio, la diferencia fundamental entre ambos es que Meltdown permite acceder a la memoria del sistema, mientras que Spectre permite acceder a la memoria de otras aplicaciones para robar esos datos.

Ya que Meltdown y Spectre son problemas de diseño en los procesadores, no es posible encontrar solución por Hardware para los procesadores existentes y dado que constantemente aparecen nuevas formas de explotar dichos fallos, la única manera de mantener el equipo de cómputo, comunicaciones y redes de internet a salvo es mediante Software que debe implementar las soluciones en los sistemas operativos. En particular en el Kernel de Linux se trabaja en parchar en cada versión del Kernel todos los fallos reportados, por esto y por otra gama de fallos e inseguridades es necesario mantener siempre el sistema operativo y sus aplicaciones actualizadas.

Como se había comentado anteriormente, estos problemas de diseño afectan a todos los procesadores Intel, AMD, IBM POWER y ARM. Eso incluye básicamente a todos los procesadores que están funcionando al día de hoy[12] en nuestros equipos, ya que estos procesadores llevan produciéndose desde 1995. Afecta a una amplia gama de sistemas.

En el momento de hacerse pública su existencia se incluían todos los dispositivos que no utilizasen una versión convenientemente parcheada de IOS, GNU/Linux, MacOS, Android, Windows y Android. Por lo tanto, muchos servidores y servicios en la nube se han visto impactados, así como potencialmente la mayoría de dispositivos inteligentes y sistemas embebidos que utilizan procesadores con arquitectura ARM (dispositivos móviles, televisores

(AC, DE, P, SM, SS, UD, GP, NM, RW, XD, BR, PK, BND), Spectre (PHT, BTB, RSB, STL, SSB, RSRE), PortSmash, Foreshadow, Spoiler, ZombieLoad (1 y 2), Kaiser, RIDL, Plundervolt, LVI, Take a Way, Collide+Probe, Load+Reload, LVI-LFB, MSD, CSME, RYZENFALL (1, 2, 3, 4), FALLOUT (1, 2, 3) , CHIMERA (FW, HW), MASTERKEY (1, 2, 3), SWAPGS, ITLB_Multihit, SRBDS, L1TF, etc. Más información en:

https://cve.mitre.org
https://meltdownattack.com/

[12] Solo en el año 2021 se detectaron 16 vulnerabilidades en procesadores INTEL y 31 en los procesadores AMD.

inteligentes y otros), incluyendo una amplia gama de equipo usado en redes. Se ha considerado que una solución basada únicamente en Software para estas fallas alenta los equipos de cómputo entre un 20 y un 40 por ciento dependiendo de la tarea que realizan y el procesador del equipo.

Memoria RAM La memoria RAM (Random Access Memory) o memoria de acceso aleatorio es un componente físico de nuestro ordenador, generalmente instalado sobre la misma placa base. La memoria RAM es extraíble y se puede ampliar mediante módulos de distintas capacidades.

La función de la memoria RAM es la de cargar los datos e instrucciones que se ejecutan en el procesador. Estas instrucciones y datos provienen del sistema operativo, dispositivos de entrada y salida, de discos duros y todo lo que está instalado en el equipo.

En la memoria RAM se almacenan todos los datos e instrucciones de los programas que se están ejecutando, estas son enviadas desde las unidades de almacenamiento antes de su ejecución. De esta forma podremos tener disponibles todos los programas que ejecutamos. Se llama memoria de acceso aleatorio porque se puede leer y escribir en cualquiera de sus posiciones de memoria sin necesidad de respetar un orden secuencial para su acceso.

De forma general existen o han existido dos tipos de memorias RAM. Las de tipo asíncrono, que no cuentan con un reloj para poder sincronizarse con el procesador. Y las de tipo síncrono que son capaces de mantener la sincronización con el procesador para ganar en eficacia y eficiencia en el acceso y almacenamiento de información en ellas. Veamos cuales existen de cada tipo.

Memorias de Tipo Asíncrono o DRAM las primeras memorias DRAM (Dinamic RAM) o RAM dinámica eran de tipo asíncrono. Se denomina DRAM por su característica de almacenamiento de información de forma aleatoria y dinámica. Su estructura de transistor y condensador hace que para que un dato quede almacenado dentro una celda de memoria, será necesario alimentar el condensador de forma periódica.

Estas memorias dinámicas eran de tipo asíncrono, por lo que no existía un elemento capaz de sincronizar la frecuencia del procesador con la frecuencia de la propia memoria. Esto provocaba que existiera menor eficiencia en la comunicación entre estos dos elementos.

Memorias de Tipo Síncrono o SDRAM a diferencia de las anteriores esta memoria RAM dinámica cuenta con un reloj interno capaz de sincronizar esta con el procesador. De esta forma se mejoran notablemente los tiempos de acceso y la eficiencia de comunicación entre ambos elementos.

Actualmente todos nuestras computadoras cuentan con memorias tipo síncrono operando en ellas. Los principales tipos de memoria son: DDR, DDR2, DDR3, DDR4 y la nueva DDR5. Donde las tasas de transferencia (GB/s) son: DDR (2.1 - 3.2), DDR2 (4.2 - 6.4), DDR3 (8.5 - 14.9), DDR4 (17 - 25.6) y DDR5 (38.4 - 51.2).

Aparte las características propias de cada una de las diferentes memorias DDR, la característica más importante es que, por ejemplo, en la memoria DDR4 cuatro cores pueden acceder simultáneamente a ella y en la DDR5 serán cinco cores.

Caché L1, L2 y L3 La memoria Caché es otra de las especificaciones importantes de los procesadores, y sirve de manera esencial de la misma manera que la memoria RAM: como almacenamiento temporal de datos. No obstante, dado que la memoria Caché está en el procesador en sí, es mucho más rápida y el procesador puede acceder a ella de manera más eficiente, así que el tamaño de esta memoria puede tener un impacto bastante notable en el rendimiento, especialmente cuando se realizan tareas que demandan un uso intensivo del CPU como en el cómputo de alto desempeño o cómputo científico.

La memoria caché se compone de RAM estática (SRAM) para mayor velocidad. La memoria SRAM es aproximadamente seis veces más grande, y suele usar seis transistores MOSFET por cada bit de memoria, que la memoria del mismo tamaño con RAM dinámica (DRAM), que usa un solo transistor MOSFET y un pequeño condensador por cada bit. Además de ocupar más espacio, la SRAM consume mucha más energía. Este mayor consumo se debe a que usa más transistores y funciona extremadamente rápido en comparación con la memoria externa. Cuanto más rápido conmutan los MOSFET, más energía consumen. Y un mayor poder conlleva... no, no una gran responsabilidad, ¡sino mucho más calor!.

Una CPU tiene limitaciones de fabricación en cuanto al tamaño del chip. El tamaño de la matriz que contiene los circuitos de la CPU es mucho menor que el del encapsulado, y gran parte del espacio se dedica a los cables que van a las conexiones. Se podría agrandar la matriz (y el encapsulado aún necesita

ser mayor para las mismas conexiones), pero el rendimiento (el porcentaje de rendimiento) disminuye considerablemente. Un menor rendimiento significa que el precio subirá... ¡y mucho!

Así que tenemos una memoria caché que queremos agrandar, pero el espacio es limitado. Y cuanta más caché tengamos, más se calentará la CPU debido a toda esa memoria caché rápida. Simplemente no se puede disipar ese calor de la CPU con la suficiente rapidez, por lo que se sobrecalentará y simplemente dejará de funcionar. Por lo tanto, debe haber un equilibrio muy cuidadoso.

Y a medida que se añade más memoria caché, no se puede acercar toda a las partes de la CPU que la usan. Por lo tanto, esta distancia adicional se traduce en un tiempo adicional para que la señal se propague a donde se necesita. La velocidad de la luz viaja a 30 cm/nanosegundo en el vacío. La velocidad de la electricidad en chips de silicio es aproximadamente un tercio de la velocidad de la luz, o 10 cm/nanosegundo. Si se trabaja a 4 GHz, eso equivale a aproximadamente 2,5 cm/seg. Y 2,5 cm/seg no es mucho, ya que las señales no necesariamente siguen una línea recta en un circuito integrado.

Este tiempo se vuelve crítico cuando se trabaja a estas altas velocidades. Esto también es lo que limita a las CPU, así como a la memoria caché, a alcanzar velocidades mucho más allá de los 5 GHz. Además, nos acercamos al mundo cuántico de la electrónica a medida que nos hacemos más pequeños, y lo que funcionaba con un tamaño de fabricación de 10 nm podría no funcionar con 3 nm, lo que requeriría muchos ajustes o una tecnología completamente nueva.

Y para quienes piensan que podemos acercar más memoria caché a la CPU construyendo capas verticales sobre ella, la respuesta es sí, es posible (y se hace en diversas memorias flash y SSD). Sin embargo, cada capa aísla las demás capas internas y, de nuevo, el calor no se puede disipar, y la CPU se sobrecalentará y simplemente dejará de funcionar. De nuevo, se trata de un equilibrio muy delicado.

Para obtener la mejor velocidad efectiva de toda la memoria principal, utilizamos un esquema de caché multinivel. La caché más pequeña (denominada nivel 1) es la más cercana a las partes importantes del procesador; cada nivel adicional se vuelve un poco más grande, pero más alejado (por lo tanto, un poco más lento). La última caché interna se conecta a la CPU para acceder a la memoria principal. Por lo tanto, si hemos realizado el diseño correctamente con el número óptimo de tamaños y niveles, la velocidad efectiva de la memoria principal funcionará cerca de la velocidad de la caché

más pequeña y rápida, y no sobrecalentaremos la CPU (con una refrigeración adecuada). La RAM actúa, mediante un programa, como caché para los SSD y los HDD, que también tienen sus propias cachés.

La Caché se divide en diferentes jerarquías de acceso:

- La Caché L1 es el primer sitio donde la CPU buscará información, pero también es la más pequeña y la más rápida, a veces para mayor eficiencia, la Caché L1 se subdivide en L1d (datos) y L1i (instrucciones), actualmente los procesadores modernos en cada core tiene su propio cache de datos e instrucciones.

- La Caché L2 suele ser más grande que la L1 pero es algo más lenta. Sin embargo, por norma general es la que mayor impacto tiene en el rendimiento, este también está incluido en cada core.

- La Caché L3 es mucho más grande que las anteriores, y generalmente se comparte entre todos los núcleos del procesador (a diferencia de las anteriores, que normalmente van ligadas a cada core). Este tercer nivel es en el que buscará el procesador la información tras no encontrarla en la L1 y L2, por lo que su tiempo de acceso es todavía mayor.

Para poner en contexto la relevancia de la memoria Caché, supongamos que el acceso a los datos de la memoria Caché L1 por el procesador es de dos ciclos de reloj, el acceso a la memoria Caché L2 es de 6 ciclos de reloj, el acceso a la memoria Caché L3 es de 12 ciclos y el acceso a la RAM es de 32 ciclos de reloj.

Además supongamos que la operación suma y resta necesitan de 2 ciclos de reloj para completar la operación una vez que cuente con los datos involucrados en dicha operación, que la multiplicación requiere 4 ciclos de reloj para completar la operación, la división necesita 6 ciclos de reloj para completar la operación y estamos despreciando el tiempo necesario para poner los datos del Caché L1 a los registros del procesador para poder iniciar el cálculo, así también despreciamos el tiempo requerido para sacar el resultado de los registros del procesador al Caché L1.

Esto nos da una idea del número máximo teórico de operaciones básicas que un procesador puede realizar por segundo dependiendo de la velocidad

de reloj de la CPU[13].

Si nosotros necesitamos hacer la multiplicación de una matriz $\underline{\underline{A}}$ es de tamaño $n \times n$ por un vector $\underline{u}$ de tamaño n y guardar el resultado en el vector $\underline{f}$ de tamaño n. Entonces algunos escenarios son posibles:

1. Si el código del programa cabe en el Caché L1 de instrucciones y la matriz $\underline{\underline{A}}$, los vectores $\underline{u}$ y $\underline{f}$ caben íntegramente en el Caché L1 de datos, entonces el procesador estará siendo utilizado de forma óptima al hacer los cálculos pues no tendrá tiempos muertos por espera de datos.

2. Si el código del programa cabe en el Caché L1 de instrucciones y los vectores $\underline{u}$ y $\underline{f}$ caben íntegramente en el Caché L1 de datos pero la matriz $\underline{\underline{A}}$ está dispersa entre los Cachés L1 y L2, entonces el procesador estará teniendo algunos tiempos muertos mientras carga la parte que necesita de la matriz del Caché L2 a L1 para hacer los cálculos y utilizado de forma óptima el procesador mientras no salga del Caché L1.

3. Si el código del programa cabe en el Caché L1 de instrucciones y los vectores $\underline{u}$ y $\underline{f}$ caben íntegramente en el Caché L1 de datos pero la matriz $\underline{\underline{A}}$ está dispersa entre los Cachés L1, L2 y L3, entonces el procesador estará teniendo muchos tiempos muertos mientras carga la parte que necesita de la matriz del Caché L3 y L2 a L1 para hacer los cálculos resultando en mediana eficiencia en el uso del procesador.

4. Si el código del programa cabe en el Caché L1 de instrucciones y los vectores $\underline{u}$ y $\underline{f}$ caben íntegramente en los Cachés L3, L2 y L1 pero los datos de la matriz $\underline{\underline{A}}$ está dispersa entre la RAM y los Cachés L3, L2 y L1, entonces el procesador estará teniendo un exceso de tiempos muertos mientras carga la parte que necesita de la matriz de la RAM a los Cachés L3, L2 y L1 para hacer los cálculos resultando en una gran pérdida de eficiencia en el uso del procesador.

[13] Por ejemplo en un procesador AMD Ryzen 9 3900X con 12 Cores (2 Threads por Core) por procesador emulando un total de 24 Cores, corre a una frecuencia base de 3,340 MHz, con una frecuencia mínima de 2,200 MHz y máxima de 4,917 Mhz, con Caché L1d de 384 KiB, L1i de 384 KiB, Caché L2 de 6 MiB y Caché L3 de 64 MiB.

Además, debemos recordar que la computadora moderna nunca dedica el cien por ciento del CPU a un solo programa, ya que los equipos son multitarea[14] y multiusuario[15] por lo que la conmutación de procesos (que se realiza cada cierta cantidad de milisegundos) degrada aún más la eficiencia computacional de los procesos que demandan un uso intensivo de CPU[16].

Last Level Cache se le llama Last Level Cache siempre al último nivel de Caché de una CPU, existen dos tipos:

- Last Level Cache Estándar.
- Victim Cache.

Una Victim Cache no actúia como la Caché de último nivel de una CPU, sino que en ese caso lo hace el penúltimo nivel y en la Victim Cache acaban los últimos datos descartados de la Caché y que han sido volcados en la RAM, los cuales son copiados en la Victim Cache para poder acceder a ellos más rápido.

[14] Cuentan con la capacidad para ejecutar varios procesos simultáneamente en uno o más procesadores, para ello necesitan hacer uso de la conmutación de tareas, es decir, cada cierto tiempo detiene el programa que está corriendo y guardan sus datos, para poder cargar en memoria otro programa y sus respectivos datos y así reiniciar su ejecución por un período determinado de tiempo, una vez concluido su tiempo de ejecución se reinicia la conmutación de tareas con otro proceso.

[15] Se refiere a todos aquellos sistemas operativos que permiten el empleo de sus procesamientos y servicios al mismo tiempo. Así, el sistema operativo cuenta con la capacidad de satisfacer las necesidades de varios usuarios al mismo tiempo, siendo capaz de gestionar y compartir sus recursos en función del número de usuarios que estén conectados a la vez.

[16] Actualmente existen una gran cantidad de distribuciones de GNU/Linux que vienen muy optimizadas intentando conseguir la mejor desenvoltura de su arquitectura y configuraciones de serie. En el caso de la configuración por omisión de Debian GNU/Linux y Ubuntu, están pensadas para que sean lo más robusta posible y que se use en todas las circunstancias imaginables, por ello están optimizadas de forma muy conservadora para tener un equilibrio entre eficiencia y consumo de energía. Pero es posible agregar uno o más Kernels GNU/Linux generados por terceros que contenga las optimizaciones necesarias para hacer más eficiente y competitivo en cuestiones de gestión y ahorro de recursos del sistema.

Hay varias opciones del Kernel GNU/Linux optimizado (Liquorix viene optimizado para multimedia y Juegos, por otro lado XanMod tiene uno para propósito general, otro aplicaciones críticas en tiempo real y otro más para cálculos intensivos) de las últimas versiones estable del Kernel.

Smart Cache la Smart Cache (o Caché) es esencialmente L3 pero optimizada por Intel para ser más eficiente a la hora de compartir la información en los núcleos de la CPU. A efectos prácticos, se comporta de igual manera que la Caché L3.

Disco Son dispositivos no volátiles (los hay del orden de hasta 32 TB y continuamente incrementan su capacidad[17]), lo que significa que retienen datos incluso cuando no tienen energía. La información almacenada permanece segura e intacta a menos que el disco duro sea destruido o interferido. La información se almacena o se recupera de manera aleatoria en lugar de acceso secuencial. Esto implica que se puede acceder a los bloques de datos en cualquier momento sin necesidad de pasar por otros bloques de datos.

Actualmente, podemos agrupar los discos duros disponibles en cuatro tipos:

- Parallel Advanced Technology Attachment (PATA)
- Serial ATA (SATA)

[17] Durante años la tecnología más popular entre los fabricantes ha sido la PMR (Perpendicular Magnetic Recording), también conocida como CMR (Conventional Magnetic Recording). A esta tecnología luego se le sumó la variante SMR (Shingled Magnetic Recording), que lograba aumentar la densidad de grabación, pero lo hacía sacrificando velocidad de transferencia y fiabilidad de las operaciones.

Western Digital ha creado la tecnología ePMR (energy-assisted Perpendicular Magnetic Recording) que permite ofrecer mayores densidades de grabación y, según este fabricante, mejorar la fiabilidad de las escrituras y evitar así los sacrificios que había que hacer con SMR (en los últimos tiempos han aparecido unidades de 20 a 32 TB basadas en dicha tecnología).

Más interesante aún es el sistema de grabación MAMR (Microwave-Assisted Magnetic Recording) que hace uso de microondas para calentar el medio de almacenamiento y así lograr mejorar densidad de grabación y fiabilidad de lecturas y escrituras. Hace años ya prometían que gracias a esta tecnología contaríamos con unidades de 40 TB en 2025, pero parece que dicho logro aún tardará en llegar.

Esta otra opción es una alternativa a las microondas, pero en HAMR (Heat-Assisted Magnetic Recording) el proceso de calentar el medio de almacenamiento lo realiza un láser. Toshiba prometió lanzar unidades de más de 32 TB en 2024, mientras que Seagate también quería ofrecer esa capacidad de forma inminente para luego dar el salto a unidades de 40 TB e incluso a los 100 TB que plantean para 2030. Ahí es donde probablemente entre en acción la evolución de HAMR+, que tratará de exprimir aún más la densidad de grabación.

- Interfaz de sistema de computadora pequeña (SCSI)
- Adjunto de tecnología avanzada paralela
- Unidades de estado sólido (SSD)

En promedio, las velocidades máximas de los discos actuales son:

- Disco SATA3 de 5,400 RPM, Lectura: 102 MB/s, Escritura: 96 MB/s
- Disco SATA3 de 7,200 RPM, Lectura: 272 MB/S, Escritura: 200 MB/s
- Disco SSD SATA, Lectura 550 MB/s, Escritura 520 MB/s
- Disco SSD NVMe, Lectura 6,600 MB/s, Escritura 5,500 MB/s
- Disco SSD PCI 5.0, Lectura 13,000 MB/s, Escritura 12,000 MB/s

En promedio, las velocidades máximas de las Unidades Flash USB[18] son:

- Unidad Flash USB 2.0, 35 MB/s
- Unidad Flash USB 3.0 o 3.1 gen 1, 5 Gbit/s
- Unidad Flash USB 3.0 o 3.1 gen 2, 10 Gbit/s
- Unidad Flash USB 3.2 gen 2x2, 20 Gbit/s

Disco de Estado Sólido SSD Estos son los últimos avances en tecnología de almacenamiento que tenemos en la industria de las computadoras. Son totalmente diferentes de las otras unidades en que no consisten en partes móviles. Tampoco almacenan datos utilizando magnetismo. En su lugar, hacen uso de la tecnología de memoria flash, circuitos integrados o dispositivos semiconductores para almacenar datos de forma permanente, al menos hasta que se borren. Estas son algunas de sus ventajas.

- Acceso a datos más rápido

[18] Los colores en los puertos USB son: USB 1.X blanco (12 Mbps), USB 2.X Negro (480 Mbps), USB 3.0 Azul oscuro (5 Gbps), USB 3.1 Azul claro (10 Gbps), USB 3.2 Rojo (20 Gbps). En el caso del USB de color Amarillo, esté es un puerto de carga aún con el dispositivo apagado.

- Menos susceptible a los golpes
- Menores tiempos de acceso y latencia
- Menos consumo de energía

Los SSD actuales están disponibles tanto en versiones SATA como en versiones M.2, U.2 y en formato de tarjeta PCI Express 4.0. Los tres últimos hacen uso del protocolo NVMe y la interfaz PCI Express 4.0 x4, lo que les permite superar los 6,600 MB/s de velocidades de lectura y escritura, frente a los 550 MB/s que suelen alcanzar como máximo las unidades SATA. La nueva versión PCI 5.0 ofrece un ancho de banda de 32 GT/s el doble de PCI 4.0, permitiendo discos SSD con 13,000 MS/s de velocidad de lectura secuencial y realizar hasta 2,500K operaciones por segundo de lectura aleatoria y tamaño máximo 15.36 TB a un precio exorbitante.

Tarjetas microSD Cuando compramos una tarjeta microSD para ampliar el almacenamiento de nuestro Smartphone, cámara, tableta o cualquier otro dispositivo electrónico la mayoría de la gente normalmente solo se fija en la capacidad de almacenamiento. Ahora bien, ¿qué significan todas esas etiquetas y nombres que llevan adscritas las microSD? ¿Cuál es la diferencia entre una microSDXC y una microSDHC? ¿Es mejor una UHS-I o una UHS-II? ¿Qué quiere decir que una tarjeta es A1 y V30? A continuación, intentamos aclarar toda esta nomenclatura.

Lo primero que tenemos que tener claro es que cuando analizamos una tarjeta micro SD existen multitud de factores que limitan su velocidad y capacidad de almacenamiento. Su rendimiento depende de factores como el tipo de tarjeta que estamos usando, su clase, y otros detalles como el tipo de bus o el número de operaciones que puede realizar por segundo.

Tipos de tarjetas microSD actualmente existen 4 generaciones distintas de tarjetas de memoria microSD. Cuanto más modernas sean, mayores velocidades y almacenamiento podrán ofrecer:

- Tarjetas micro SD (Secure Digital): Estas son las memorias de primera generación. Las desarrolló el fabricante SanDisk y fueron las primeras en utilizar el formato de 15 x 11 x 1 milímetros. Su capacidad máxima es de 32 GB.

- Tarjetas micro SDHC (Secure Digital High Capacity): Tarjetas de segunda generación. Cuentan con un bus de datos mejorado que permite alcanzar velocidades superiores, aunque su capacidad máxima sigue siendo de 32 GB.
- Tarjetas micro SDXC (Secure Digital Extended Capacity): Estas micro SD utilizan un sistema de archivos exFAT y su velocidad de transferencia puede llegar hasta los 312 MB/s. Su capacidad de almacenamiento puede llegar hasta los 2 TB y es el tipo de tarjeta más común utilizado a día de hoy.
- Tarjetas micro SDUC: Estas son las tarjetas de memoria más modernas y punteras. Utilizan el sistema de archivos exFAT y permiten almacenar entre 2 TB y 128 TB de datos.

Evidentemente con esto no es suficiente. Si queremos tener una idea aproximada de la velocidad de la micro SD tendremos que fijarnos en aspectos como la clase y tipo de bus que emplea.

La clase es una característica que nos indica la velocidad de transferencia de datos mínima de la tarjeta de memoria. Actualmente hay 4 tipos de clase diferentes:

- Clase 2: Velocidad mínima de 2 MB/s
- Clase 4: Velocidad mínima de 4 MB/s
- Clase 6: Velocidad mínima de 6 MB/s
- Clase 10: Velocidad mínima de 10MB/s

Hoy en día la mayoría de tarjetas micro SD son de clase 10, ya que son capaces de transferir más de 10 MB/s y superan esa cifra fácilmente.

El bus determina la velocidad de la interfaz de la tarjeta de memoria, y nos puede servir como indicativo para conocer la rapidez con la que se pueden leer y escribir los datos:

- Bus estándar: Su velocidad de transferencia alcanza hasta los 12.5 MB/s. Es el tipo de bus utilizado en tarjetas de clase 2, 4 y 6.
- Bus de alta velocidad (High Speed): Se utiliza en tarjetas de clase 10 y alcanza una velocidad de hasta 25 MB/s.

- Bus Ultra High Speed (UHS): Estos son los buses con la interfaz más rápida, y existen varios tipos:
  - UHS-I: Hay dos tipos de buses UHS-I. Por un lado, tenemos el UHS-I clase 1 (U1) que alcanza velocidades de 50 MB/s. Y luego tenemos el UHS-I clase 3 (U3) que llega hasta los 104 MB/s.
  - UHS-II: Alcanza velocidades de transferencia hasta 312 MB/s.
  - UHS-III: Velocidades de transferencia de datos que alcanzan hasta los 624 MB/s.
- SD-Express: Este es el tipo de bus más potente de todos, llegando hasta los 985 MB/s.

Como referencia, te interesará saber que actualmente la mayoría de tarjetas micro SD de gama media utilizan un bus UHS-I de clase 3 (U3) con velocidades de lectura de hasta 104 MB/s.

Otro factor importante es la velocidad de lectura y escritura aleatoria (IOPS) u operaciones por segundo que puede realizar una tarjeta. Este dato determina el rendimiento mínimo en la lectura y escritura aleatoria de la SD:

- Clase de rendimiento de aplicación A1: Las tarjetas A1 tienen una velocidad mínima de lectura aleatoria de 1,500 IOPS, y una velocidad mínima de escritura aleatoria de 500 IOPS.
- Clase de rendimiento de aplicación A2: Las tarjetas A2 ofrecen velocidades superiores, con 4,000 IOPS de lectura y 2,000 IOPS de escritura.

Normalmente con una tarjeta A1 es más que suficiente para tareas del día a día, aunque si necesitamos un rendimiento superior, por ejemplo, para ejecutar aplicaciones desde la SD o jugar a videojuegos, las tarjetas A2 ofrecen un mejor rendimiento.

La velocidad de escritura aleatoria (A1 y A2) es un dato relevante para los Smartphones y tabletas, pero si tenemos una cámara de grabación, una Action camera o un Dron, la característica en la que nos tenemos que fijar es en el Velocidad de escritura secuencial (sistema V) que utiliza (en inglés, Video Speed Class). O dicho de otra forma, en su velocidad de escritura secuencial.

Esta característica nos indica la cantidad de datos que se pueden grabar en la micro SD de forma constante sin bajar de una velocidad mínima. Esto resulta esencial cuando queremos grabar vídeos en alta y ultra-alta definición:

- V30 (Video Speed Class 30): Velocidad de escritura mínima de 30 MB/s
- V60 (Video Speed Class 60): Velocidad de escritura mínima de 60 MB/s
- V90 (Video Speed Class 90): Velocidad de escritura mínima de 90 MB/s

Por ejemplo, si vamos a grabar vídeo en resolución 4K directamente en la tarjeta micro SD, es necesario que la velocidad V sea lo máximo posible, especialmente si vamos a utilizar un amplio BitRate con bajos niveles de compresión, o calidades superiores como el 8K.

Cintas Magnéticas En el año 2010, se comunicó que todos los datos utilizados para el proyecto del satélite Nimbus se recuperaron de cintas que en ese momento tenían 46 años. A partir de dicho comunicado se extendió el uso de la cinta magnética para almacenamiento de datos en todo el mundo.

En un mundo altamente digital, la cinta magnética es una de las pocas tecnologías que utiliza señales analógicas para mover parte de los datos, en su esencia, la cinta se parece mucho a un HDD, utiliza materiales de base magnética, pero en este caso, la cinta es literalmente una base de material generalmente nailon que tiene un revestimiento magnético. Y en lugar de un disco giratorio, la cinta entra, está enhebrada. Puede parecer una cinta VHS, pero es mucho más robusta.

La cinta se mueve linealmente hacia la unidad de cinta y hacia el cartucho de cinta. Para escribir, el cabezal de la cinta toma señales electrónicas y crea un mini campo magnético que puede cambiar la polaridad del material de la película para formar un patrón de ceros y unos. Una vez que los datos se escriben en la cinta, no se pueden cambiar (pero se pueden borrar y reescribir).

La inmutabilidad y las capacidades de encriptación de la cinta, así como la simplicidad de crear un espacio para almacenarla en una bóveda hacen de la cinta un arma clave para asegurar que los datos sobrevivan frente al Ransomware. Uno de los grandes productores de cintas en la actualidad es IBM, los cuales argumentan que esta función hace que la cinta sea el medio ideal para almacenar datos de archivo a los que no es necesario acceder con frecuencia.

La cinta también puede servir como una copia de seguridad y de versiones fuera de línea de archivos importantes o confidenciales que son resistentes a los ataques cibernéticos. Los tipos de datos que permanecen en la cinta abarcan registros financieros, registros médicos, información de identificación personal y documentos que forman parte de una retención legal de múltiples gobiernos.

Una sola cinta mide aproximadamente 3 pulgadas por 3 pulgadas y 3/4 de pulgada de grosor. Es más pequeño que una unidad de disco duro (HDD), pero pesa alrededor de 0.6 kilogramos. Un cartucho puede almacenar 18 Terabytes de datos sin comprimir y 45 Terabytes comprimidos. IBM está trabajando para duplicar esta capacidad en la próxima generación de la tecnología. En cuanto a la velocidad de recuperación, se obtiene un flujo de datos de una unidad de cinta de 1,000 Megabits por segundo, comprimidos.

Una biblioteca de cintas puede variar en tamaño desde algo que puede poner en su escritorio hasta algo que es del tamaño de un refrigerador pequeño (alrededor de 8 pies cuadrados). La pequeña biblioteca del tamaño de un refrigerador tiene capacidad para 1584 cartuchos. IBM promociona que su biblioteca Diamondback será la biblioteca de cintas más densa del mercado. Podrá contener 69 Petabytes de información mientras ocupa menos de 8 pies cuadrados de espacio.

La cinta magnética supera al disco duro y al flash en cuanto a longevidad, costo financiero y costo de huella de carbono, pero pierde en velocidad de acceso. Las cintas no son recomendables para poner datos de producción en vivo o incluso copias de seguridad, pero son perfectas para cualquier información a la que se acceda con poca frecuencia y que deba conservarse durante mucho tiempo, como registros médicos o datos de archivo.

Es conocido que muchas empresas han usado y seguirán usando cinta magnética en sus operaciones, entre las que destacan las hiperescalas (empresas que han crecido tanto que ofrecen sus propias infraestructuras o tienen datos masivos como resultado de su infraestructura) siempre necesitan muchas formas diferentes de tecnología para manejar la variedad de datos que ingresan a sus sistemas para alimentar una gama de servicios. Entre otras destacan: Bancos, Gobiernos, Milicia y organizaciones como CERN, así como corporaciones como Amazon, Google, Meta, Baidu, Alibaba y Tencent.

Tarjeta Gráfica La tarjeta gráfica o tarjeta de vídeo es un componente que viene integrado en la placa base de la computadora o se instala aparte

para ampliar sus capacidades. Concretamente, esta tarjeta está dedicada al procesamiento de datos relacionados con el vídeo y las imágenes que se están reproduciendo en la computadora.

Procesador Gráfico GPU el corazón de la tarjeta gráfica es la GPU o Unidad de procesamiento gráfico, un circuito muy complejo que integra varios miles de millones de transistores diminutos y puede tener desde uno a miles de núcleos (ya es común encontrar computadoras personales con tarjeta de 10496 cores y 24 GB de GRAM) que tienen capacidad de procesamiento independiente. De la cantidad y capacidad de estos núcleos dependerá la potencia.

Así como los procesadores centrales de las CPU, están diseñados con pocos núcleos pero altas frecuencias de reloj, las GPU tienden al concepto opuesto, contando con grandes cantidades de núcleos con frecuencias de reloj relativamente bajas. Luego tienes la memoria gráfica de acceso aleatorio o GRAM, que son Chips de memoria que almacenan y transportan información entre sí. Esta memoria no es algo que vaya a determinar de forma importante el rendimiento máximo de una tarjeta gráfica, aunque si no es suficiente puede acabar lastrando y limitando la potencia de la CPU.

La idea de usar esa potencia para otros menesteres se denomina GPGPU (General Purpose Computation on Graphics Processing Units) o GPU Computing. En el momento en el que las tarjetas gráficas permiten que se programen funciones sobre su Hardware se empieza a hacer uso de GPGPU. Al principio era necesario utilizar los lenguajes enfocados a la visualización en pantalla (como OpenGL) para realizar otros cálculos no relacionados con los gráficos. Esto implicaba el uso de funciones muy poco flexibles, originalmente diseñadas para otros fines, lo que hacía que la labor de programar para tal fin fuese realmente tediosa y complicada.

Para facilitar el empleo de las tarjetas gráficas para cualquier uso no vinculado con los gráficos, NVidia desarrolló toda una tecnología alrededor de la tarjeta, que permitía usar la misma para cualquier tarea: CUDA. ATI, la principal (y actualmente casi única) competidora, un poco más tarde haría lo propio lanzando su propia tecnología: Stream. En un principio las tarjetas gráficas solo trabajaban con aritmética de 32 bits, pero en la actualidad ya se cuenta con aritmética de 64 bit (para lograr esto, muchas tarjetas usan dos de sus cores de 32 bits para emular uno de 64 bits, reduciendo su número de cores útiles a la mitad).

Procesador Gráfico Integrado muchos procesadores CPU incorporan una o más GPU en su interior, llamada gráfica integrada (iGPU Integrated Graphics Processing Units o APU Accelerated Processing Unit). Generalmente es muy poco potente, pero lo suficiente para realizar tareas básicas como navegar por Internet, ver vídeos, e incluso para algunos juegos básicos, especialmente en las últimas generaciones puesto que cada vez son más potentes. No obstante, en las últimas generaciones de procesadores cada vez se están introduciendo gráficos integrados más potentes, y ya son capaces de manejar varios monitores, resoluciones 4K e incluso son capaces de mover algunos juegos a una tasa digna de FPS.

Tarjeta Gráfica por ejemplo, la tarjeta gráfica de AMD Instinct MI200 cuenta con más de 200,000 cores y 128 GB de HBM2, NVidia GEFORCE RTX 3090 proporciona 10,496 cores y 24 GB de GDDR6x, NVidia A100 cuenta con 80 GB de memoria HBM2 6192 cores y 432 núcleos tensor[19], mientras que la tarjeta NVidia Titan RTX proporciona 130 Tensor TFLOP de rendimiento, 576 núcleos tensores y 24 GB de memoria GDDR6.

Por otra parte, Intel ha desarrollado una aceleradora gráfica Artic Sound-M pensada para centro de datos (especialmente diseñada para juegos en la nube) que utiliza una GPU DG2 Xe-HPG que viene con una configuración de 512 unidades de ejecución lo que equivale a 4,096 Shaders, por ejemplo, esta aceleradora puede manejar hasta 8 Streamings simultáneos de video 4K o más de 30 si el vídeo es en 1080p y cuenta con más de 60 funciones virtualizadas.

En agosto del 2021, se anunció la construcción de la supercomputadora Polaris, acelerado por 2240 GPU NVIDIA A100 Tensor Core, el sistema puede alcanzar casi 1.4 exaflops de rendimiento teórico de IA y aproximadamente 44 petaflops de rendimiento máximo de doble precisión. Polaris, que será construido por Hewlett Packard Enterprise, combinará simulación y aprendizaje automático al abordar cargas de trabajo informáticas de alto rendimiento de inteligencia artificial y con uso intensivo de datos, impulsadas por 560 nodos en total, cada uno con cuatro GPU NVIDIA A100.

Tipos de Redes Según el Medio Físico Si bien, nuestros dispositivos de cómputo pueden funcionar sin conexión de red, estos se ven inmediatamente

[19] Un Tensor core (o núcleos Tensor) calculan la operación de una matriz 4x4 completa, la cual se calcula por reloj. Estos núcleos pueden multiplicar dos matrices FP16 4x4 y sumar la matriz FP32 al acumulador.

limitados. La red nos permite conectarnos a Internet que es el camino por el cual nos conectamos con el mundo. Las formas de conectar nuestros equipos a Internet en un principio fue exclusivamente por red alámbrica, desde ya hace unos años a la fecha se dispone de conexión a red alámbrica e inalámbrica, pero actualmente nuestros dispositivos cuentan casi exclusivamente con conexión inalámbrica.

¿Qué es el ancho de banda? Se trata de la capacidad máxima y la cantidad de datos que se pueden transmitir a través de una conexión (de internet, por ejemplo), en un momento determinado. Algo que debemos tener claro es que el ancho de banda de red es fundamental para la calidad y velocidad de la conexión.

El ancho de banda se mide en *bit/s* o en sus múltiplos *k/bits* o *m/bits* por segundo. Y para la mayoría de los casos, debemos asegurarnos siempre de tener el mayor ancho de banda que nos sea posible, porque de esta manera podremos tener una mejor y más rápida transferencia de datos.

¿Qué es entonces la velocidad de transmisión? Este término se puede definir como la velocidad a la que se transmite la información. Cuando un usuario adquiere un paquete con una empresa prestadora de servicios de internet, recibe, por ejemplo, 10 mbps, 30 mbps, 100 mbps, etc. Y esto se refiere a la cantidad de datos que podemos descargar o subir a la red. Como recomendación, lo indicado es que para que la velocidad pueda existir será necesario tener un ancho de banda igual o superior a la velocidad contratada en el paquete de servicio.

Normalmente vemos en los anuncios de todos los operadores, que estos ofrecen una cantidad cualquiera de megas de navegación; este valor numérico corresponde a la velocidad de descarga únicamente. Para encontrar la velocidad de subida, es necesario acceder a un test que nos revele cuál es el resultado y si lo que nos prometen, es verdad o no.

¿Qué es la latencia? Es el tiempo total que transcurre desde que enviamos una información, hasta que la misma llega a un receptor. Su valor de medición se hace en milisegundos, también se conoce como *Ping* y está presente en actividades que realiza cotidianamente como jugar en línea o hacer videollamadas.

¿Altera la latencia la velocidad de la conexión? La velocidad de conexión influye en la latencia una vez que pasamos de un rango predeterminado. Poniéndolo en un ejemplo, si tenemos una conexión a Internet de 1 Mbps y la comparamos con una conexión de 100 Mbps, dependiendo del tamaño del paquete se notará una mejora grande en la velocidad. Otros factores que importan a la hora de hablar de latencia son el estar conectado a internet por Wi-fi o un cable, si tiene servicio de fibra óptica o qué tanta distancia hay entre su ordenador y un Router, etc.

La latencia en la conexión también es la suma de otros retardos:

- De procesamiento: se define en el tiempo que tardan los Routers en examinar la cabecera y a su vez, la respuesta en determinar a dónde hay que enviar cualquier paquete haciendo una previa comprobación de sus tablas de enrutamiento.
- De cola: tiempo de espera del paquete para poder ser transmitido a través de un enlace físico. Cabe anotar que no podemos saber previamente si va a haber un retardo de cola o no, ya que este cambia en tiempo real.
- De transmisión: es el tiempo que tarda el paquete en arribar hasta el siguiente nodo o destino final.
- De propagación: es el tiempo que tarda un bit en propagarse desde un punto cualquiera de origen hasta llegar a uno de destino. Su velocidad depende del medio físico por el que se transporte.

El retardo total es la suma de todos los retardos anteriormente enunciados.

Comúnmente se asocia la latencia con la banda de ancha, pero existe una diferencia sustancial entre ambas. Si bien ambas afectan la velocidad de la conexión, la banda ancha permite que se pueda transmitir una gran cantidad de datos, mientras la latencia determina a qué velocidad se transmite esa cantidad de datos.

Si bien, tener red nos permite estar conectados, tenemos una gran limitación por las velocidades de conexión a las que tendremos acceso según el tipo de medio físico que usemos para conectarnos, así como el número de dispositivos con los que compartamos la conexión. Las redes inalámbricas parecen ser omnipresentes, pero las velocidades de interconexión dejan mucho que desear como veremos a continuación.

Redes alámbricas se comunica a través de cables de datos (generalmente basada en Ethernet). Los cables de datos, conocidos como cables de red de Ethernet o cables con hilos conductores (CAT5), conectan computadoras y otros dispositivos que forman las redes. Las redes alámbricas son mejores cuando se necesita mover grandes cantidades de datos a altas velocidades, como medios multimedia de calidad profesional.

Ventajas

- Costos relativamente bajos
- Ofrece el máximo rendimiento posible
- Mayor velocidad - cable de Ethernet estándar hasta 1 Gbps[20]
- Mayor rendimiento de Voz sobre IP.
- Mejores estándares Ethernet en la industria.
- Mayor capacidad de ancho de banda por cables.
- Aplicaciones que utilizan un ancho de banda continúo.

Desventajas

- El costo de instalación siempre ha sido un problema común en este tipo de tecnología, ya que el estudio de instalación, canaletas, conectores, cables y otros suman costos muy elevados en algunas ocasiones.
- El acceso físico es uno de los problemas más comunes dentro de las redes alámbricas. Ya que para llegar a ciertos lugares, es muy complicado el paso de los cables a través de las paredes de concreto u otros obstáculos.
- Dificultad y expectativas de expansión es otro de los problemas más comunes, ya que cuando pensamos tener un número definido de nodos en una oficina, la mayoría del tiempo hay necesidades de construir uno nuevo y ya no tenemos espacio en los Switches instalados.

[20] El término bps se refiere a transmitir Bits por segundo (se requieren 8 Bits para formar un Byte). Por eso el término de 1,000 Mbps es equivalente a 125 MB/s.

Hoy en día se puede hacer la siguiente clasificación de las redes de protocolo Ethernet para cable y fibra óptica[21]:

- Ethernet, que alcanza no más de 10 Mbps de velocidad
- Fast Ethernet, que puede trabajar con hasta 100 Mbps
- Gigabit Ethernet, alcanza hasta 1 Gbps (1000 Mbps aprox.)
- 2.5 y 5 Gigabit Ethernet hasta 2.5 Gbps si usamos cableado Cat 5a y nada menos que 5 Gbps con cableado Cat 6
- 10 Gigabit Ethernet, que puede alcanzar hasta los 10 GMbps
- 1000GbE para alcanzar la Ethernet Terabit (125 Gbytes)

La categoría del cable o el tipo de fibra óptica determina la velocidad máxima soportada por cada tipo de cable, pero aunque haya cables con la misma velocidad hay otros factores que determinan su usabilidad, como el ancho de banda o la frecuencia. La frecuencia o ancho de banda determina la potencia de la red, a mayor frecuencia mayor ancho de banda y menor perdida de datos. Este factor es importante si vamos a conectar varios equipos al mismo cable de red o vamos a hacer una gran tirada de cable, ya que cuanto más largo sea el cable de red más potencia perderá. Siempre tendrá más velocidad un cable corto que un cable largo, pero si el ancho de banda es amplio tardará más metros en perder potencia y velocidad.

[21] El récord mundial en mayo del 2022 de transmisión en fibra óptica es de 1.02 petabits por segundo enviados a través de 51.7 kilómetros (que podría transmitir hasta 10 millones de canales por segundo de vídeo a resolución 8K), que rompe al récord anterior de 319 terabits por segundo sobre una distancia de 1,800 millas (con el estimado de descarga de 80,000 películas simultáneamente en un segundo).

En 2023 los investigadores de Electronics and Computer Engineering de Aston University en U.K. alcanzaron una velocidad de 301 terabits por segundo (Tbps), equivalente a transferir 1,800 películas 4K a través de Internet en un segundo, utilizando cables de fibra óptica existentes. En comparación, la velocidad media de banda ancha fija en los EE. UU. es de 242,38 megabits por segundo (Mbps), según Speed Test.

Los resultados de la prueba, que se realizaron utilizando el tipo de cables de fibra ya tendidos en el suelo, lograron esta velocidad vertiginosa enviando luz infrarroja a través de hilos tubulares de vidrio, que es como funciona generalmente la banda ancha de fibra óptica. Pero aprovecharon una banda espectral que nunca se ha utilizado en sistemas comerciales, llamada "banda E", utilizando dispositivos nuevos hechos a medida.

Ethernet es el estándar que domina la gran mayoría de mercado, presente de manera casi exclusiva tanto en mercado doméstico, como en pequeña y mediana empresa representa también un porcentaje muy significativo en grandes centros de datos. Pero existen otros protocolos que se pueden situar en el mismo nivel de calidad que Gigabit Ethernet como InfiniBand.

InfiniBand es un bus serie bidireccional de comunicaciones de alta velocidad en las que las rápidas comunicaciones entre servidores son críticas para el rendimiento, llegando a ofrecer velocidades de hasta 2.0 Gbps netos en cada dirección del enlace en un nodo simple, 4 Gbps netos en un nodo doble y hasta 8 Gbps netos en un nodo quadruple. Estos nodos a su vez se pueden agrupar en grupos de 4 ó 12 enlaces llegando a velocidades de hasta 96 Gbps netos en un grupo de 12 nodos cuádruples. El factor de velocidad neta viene relacionado con que Infiniband de cada 10 bits que transmite 8 de ellos son datos, basándose en la codificación 8B/10B.

Recientemente se han implementado sistemas en los que ya no se utiliza esta codificación 8B/10B sino la 64B/66B que permite mejorar el porcentaje de datos útiles por trama enviada y que ha permitido los nodos FDR-10 (Fourteen Data Rate-10 a 10 Gbps), FDR (Fourteen Data Rate a 13.64 Gbps) y EDR (Enhanced Data Rate a 25 Gbps). Este último en un grupo de 12 nodos proporciona hasta 300 Gbps. Los últimos desarrollos de Gigabit Ethernet, proporcionan hasta 100 Gbps por puerto.

Estas enormes velocidades de conexión hacen que Infiniband sea una conexión con una muy importante presencia en superordenadores y clústers, por ejemplo del top 500 de superordenadores en 2020, 226 están conectados internamente con Infiniband, 188 lo están con Gigabig Ethernet y el resto con Myrinet, Cray, Fat Tree u otras interconexiones a medida.

Una de las principales ventajas de Infiniband sobre Ethernet es su bajísima latencia, por ejemplo y basándonos en los datos del estudio de Qlogic "Introduction to Ethernet Latency, an explanation to Latency and Latency measurement", la latencia en 10 Gpbs Ethernet se sitúa en 5 microsegundos mientras que la de Infiniband se sitúa por debajo de los 3 microsegundos.

Los sistemas de conmutadores inteligentes InfiniBand de NVIDIA Mellanox ofrecen el mayor rendimiento y densidad de puertos para computación de alto rendimiento (HPC), IA, Web 2.0, Big Data, nubes y centros de datos empresariales. La compatibilidad con configuraciones de 36 a 800 puertos a hasta 200 Gpbs por puerto permite que los clústeres de cómputo y los centros de datos convergentes funcionen a cualquier escala, lo que reduce los costos operativos y la complejidad de la infraestructura.

Redes inalámbricas: es una red en la que dos o más terminales (ordenadores, tabletas, teléfonos inteligentes, etc.) se pueden comunicar sin la necesidad de una conexión por cable. Se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros.

Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar porta cables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.

Tipos de redes inalámbricas

- LAN Inalámbrica: Red de área local inalámbrica. También puede ser una red de área metropolitana inalámbrica.
- GSM (Global System for Mobile Communications): la red GSM es utilizada mayormente por teléfonos celulares.
- D-AMPS (Digital Advanced Mobile Phone Service): está siendo reemplazada por el sistema GSM.
- Fixed Wireless Data: Es un tipo de red inalámbrica de datos que puede ser usada para conectar dos o más edificios juntos para extender o compartir el ancho de banda de una red sin que exista cableado físico entre los edificios.
- Wi-Fi[22]: es uno de los sistemas más utilizados para la creación de redes

[22]Notemos que una conexión de WiFi tradicional sin obstáculos con una intensidad de banda de 2.4 GHZ puede tener un alcance máximo de 46 metros y para la banda de 5.0 GHz un alcance de 15 metros. Paro hay muchos objetos que interfieren con la señal del Router del WiFi y el sitio en el que colocamos nuestro dispositivo inalámbrico como computadora o teléfono inteligente:

- Superficies y/o objetos de metal o vidrio blindado
- Refrigeradores, lavadoras y radiadores
- Hornos de microondas, cámaras Web, monitores de bebés y teléfonos inalámbricos
- Paredes y muros
- Dispositivos arquitectónicos que funciones como una jaula de Faraday (es un contenedor recubierto por materiales conductores de electricidad como mallas metálicas,

inalámbricas en computadoras, permitiendo acceso a recursos remotos como internet e impresoras. Utiliza ondas de radio.

Ventajas

- La instalación de redes inalámbricas suele ser más económica.
- Su instalación también es más sencilla.
- Permiten gran alcance; las redes hogareñas inalámbricas suelen tener hasta 100 metros desde la base transmisora.
- Permite la conexión de gran cantidad de dispositivos móviles. En las redes cableadas mientras más dispositivos haya, más complicado será el entramado de cables.
- Posibilidad de conectar nodos a grandes distancias sin cableado, en el caso de las redes inalámbricas corporativas.
- Permiten más libertad en el movimiento de los nodos conectados, algo que puede convertirse en un verdadero problema en las redes cableadas.
- Permite crear una red en áreas complicadas donde, por ejemplo, resulta dificultoso o muy caro conectar cables.

Desventajas

- Calidad de Servicio: La velocidad que posee la red inalámbrica no supera la cableada, ya que esta puede llegar a los 10 Mbps, frente a 100 Mbps que puede alcanzar la cableada. Hay que tomar en cuenta la tasa de error debida a las interferencias.

papel aluminio, cajas o cestos de basura de acero que funciona como un blindaje contra los efectos de un campo eléctrico proveniente del exterior).

En caso de que varios dispositivos se conecten a la red, se puede optar por colocar el Router en un punto medio, para que ninguna zona quede sin cobertura. Por otra parte, para una mejor conexión, también procura que el Router se encuentre en una zona elevada, pues esto mejorará el alcance de la señal inalámbrica. Una excelente opción para mejorar la calidad del internet inalámbrico cuando hay obstáculos es utilizar un repetidor de WiFi, este dispositivo es muy útil para amplificar la señal y llevarla a más sitios de nuestra red.

- Costo: En algunos casos, puede ser más barato cablear una casa/oficina que colocar un servicio de red inalámbrica.
- La señal inalámbrica puede verse afectada e incluso interrumpida por objetos, árboles, paredes, espejos, entre otros.

La velocidad máxima de transmisión inalámbrica de la tecnología 802.11b es de 11 Mbps. Pero la velocidad típica es solo la mitad: entre 1.5 y 5 Mbps dependiendo de si se transmiten muchos archivos pequeños o unos pocos archivos grandes. La velocidad máxima de la tecnología 802.11g es de 54 Mbps. Pero la velocidad típica de esta última tecnología es solo unas 3 veces más rápida que la de 802.11b: entre 5 y 15 Mbps. Resumiendo, las velocidades típicas de los diferentes tipos de red son:

Estándar	V.Máxima	V.Practica	Frecuencia	Ancho Banda	Alcance
802.11	2Mbit/s	1Mbit/s	2.4Ghz	22MHz	330 metros
802.11a(WiFi5)	54Mbit/s	22Mbit/s	5.4Ghz	20MHz	390 metros
802.11b	11Mbit/s	6Mbit/s	2.4Ghz	22MHz	460 metros
802.11g	54Mbit/s	22Mbit/s	2.4Ghz	20MHz	460 metros
802.11n	600Mbit/s	100Mbit/s	2.4Ghzy5.4Ghz	20 y 40MHz	820 metros
802.11ac	6.93Gbps	100Mbit/s	5.4Ghz	80 o hasta 160MHz	Poco alcance, pero sin interferencias
802.11ad	7.13Gbit/s	Hasta6Gbit/s	60Ghz	2MHz	300 metros
802.11ah	35.6Mbps	26.7Mbps	0.9Ghz	2MHz	1000 metros
802.11ax(WiFi6)	9,6Gbps	6,9Gbps	2.4Ghz y 5.4Ghz	20MHz	1000 metros

Como puedes ver, los principales factores que influyen en la calidad de una conexión WiFi, son la frecuencia, el ancho de banda y el alcance total. Considerando que, todo esto junto con la velocidad máxima y la velocidad práctica, se congregan en lo que es cada versión de este tipo de conexión a la red. Además, la conexión se degradará inexorablemente con la cantidad de dispositivos conectados y su consumo de datos.

Velocidad de los Proveedores cuando se contrata el servicio de internet, la velocidad de interconexión del mismo depende de cuánto sea el cobro, pero en la mayoría de los casos se tendrá una velocidad de descarga mayor a la velocidad de carga y nuestra red será una intranet (dirección de IP dinámica) compartida con otros miles de usuarios abonados al servicio de internet del proveedor. También es posible contratar una interconexión con

velocidades homogéneas para carga y descarga dedicada, el costo del mismo se puede hasta triplicar con respecto a uno no homogéneo.

En caso de requerir una dirección de internet homologada o pública, el costo de contratar el servicio aumenta considerablemente, pero de esta forma nuestros equipos son visibles en el Internet (esto conlleva un aumento de riesgos al estar nuestros equipos más vulnerables a ataques informáticos).

El Tráfico Global en Internet El tráfico en Internet a nivel global sigue creciendo de manera vertiginosa. Sólo en 2024 aumentó un 17.2%, según los datos del informe de 2024 Cloudflare Radar Year in Review, publicado por la compañía por quinto año consecutivo, y en el que se repasa información sobre conectividad, seguridad, uso de dispositivos para acceso a la Red y frecuencia de los apagones, entre otras tendencias.

Según este informe, y para sorpresa de prácticamente nadie a estas alturas, los servicios de Internet más populares del mundo son Google, Facebook, Apple, TikTok y AWS. Chrome, con un 65.8% de los internautas como usuarios, es el navegador más utilizado en todo el mundo. WhatsApp sigue siendo la aplicación de mensajería más popular.

React, PHP y JQuery están entre las tecnologías para desarrollar webs más populares. HubSpot, Google y WordPress están entre los proveedores más populares de servicios y plataformas de soporte. Además, Go, ha superado a NodeJS como lenguaje más popular para hacer peticiones de API automatizadas.

Los rastreadores de IA son una gran fuente de tráfico, aunque despiertan cada vez más suspicacias por su actividad. Básicamente, se dedican a escanear la web para recopilar grandes cantidades de datos para entrenar modelos grandes de lenguaje. Preocupa bastante el hecho de que algunos recojan datos sin que tengan permiso para hacerlo, frente a los bots «buenos» y verificados, que suelen tener su origen en los motores de búsqueda y son transparentes sobre lo que son y lo que hacen. En este grupo entran GoogleBot, Qualys o BingBot.

Cloudflare, entre otras actividades, se dedica a rastrear el tráfico relacionado con la IA para determinar qué bots son los más agresivos, cuáles tienen el mayor volumen de peticiones y cuáles hacen rastreos de manera regular. Según los investigadores que han realizado el informe, el denominado facebookexternalhit es el que más tráfico de todos ha generado durante el año: un 27.16%. Le siguen Bytespider, de ByteDance, con un 23.35%; Ama-

zonbot, con un 13.34%, ClaudeBot, de Anthropic, con un 8.06%; y GPTBot, con un 5.60%.

Al parecer, el tráfico generado por Bytespider, bot del propietario de TikTok, ha ido descendiendo de manera gradual durante 2024. En las semanas finales del año generaba entre un 80% y un 85% menos de tráfico que al principio. Mientras tanto el de ClaudeBot registró una subida muy pronunciada hacia mitad de 2024, y luego cayó otra vez de forma brusca.

La mayoría de las peticiones Web son todavía de HTTP2, que se lanzó en 2015, y cuenta aún con un 49.6% de las mismas. Un 29.9% todavía son de HTTP original, estandarizado en 1996, mientras que solo un 20.5% son de HTTP3, desplegado en 2022.

Cloudflare también registra, además del tráfico HTTP, las conexiones realizadas a través del protocolo de transmisión TCP, que asegura que hay una transferencia de datos fiable entre dispositivos de red. En 2024, un 20.7% de las conexiones TCP finalizaron de manera inesperada antes de que pudiesen terminar en un intercambio de datos útiles.

Estas anomalías en las conexiones TCP pueden deberse a varios motivos. Entre ellos a los ataques de denegación de servicio (DoS), al escaneado de redes, a las desconexiones de clientes, a la manipulación de las conexiones o a lo que Cloudflare ha llamado «comportamiento poco habitual del cliente».

La mayor parte de las interrupciones de una conexión TCP identificadas por Cloudflare se produjeron en 2024 después de que un servidor recibiese una petición de sincronización, pero antes de que recibiese un reconocimiento de la misma.

En cuanto a la seguridad, Cloudflare ha señalado que sólo un 4.3% de los mensajes de correo electrónico enviados en 2024 eran maliciosos. En estos había sobre todo enlaces falsos (42.9%) o identidades falsas (35.1%). En el 70% de los casos se utilizaban los dos métodos.

Como datos curiosos en cuanto a seguridad, la compañía asegura que la vulnerabilidad Log4j todavía se usa como método de ataque, y se usa de manera mucho más activa que otras vulnerabilidades comunes. Además, prácticamente todos los mensajes de correo procesados por Cloudflare con dominios .bar, .rest y .uno eran o correos de Spam, o mensajes que, directamente, eran maliciosos.

En 2024, por otro lado, hubo 225 apagones de Internet de gran envergadura. La mayoría se dieron en África, Oriente Medio o India. Más de la mitad fueron apagones ordenados directamente por gobiernos, mientras que otros se debieron a otras causas.

Entre ellas, corte de cables, apagones eléctricos, problemas técnicos o de mantenimiento, episodios climáticos graves o ciberataques. Muchos duraron solo unas pocas horas, mientras que otros, como el experimentado en Bangladesh en julio, duró 10 días. Dentro de estos apagones está también el provocado por el incidente de CrowdStrike el pasado verano.

Otro de los aspectos tratados en el informe es la calidad de la conexión a Internet de los países, con base en su velocidad de subida, la de bajada y su latencia. España, con una velocidad de descarga media de 292.6 Mbps, y de 192.6 Mbps de subida, está a la cabeza en velocidad de conexión. Todos los países desarrollados presentan velocidades de descarga por encima de 200 Mbps de media.

Un 41.3% del tráfico de Internet a nivel mundial procede de dispositivos móviles, con el otro 58.7% producido en ordenadores portátiles y de sobremesa. Eso sí, en alrededor de un centenar de países del mundo, la mayoría del tráfico en 2024 procede de dispositivos móviles. Cuba y Siria tienen el mayor tráfico de dispositivos móviles, un 77%.

Otras áreas de alta demanda de tráfico de dispositivos de este tipo son Oriente Medio, África, Asia-Pacífico y América Central y del Sur. En este aspecto, las mediciones del tráfico son parecidas a las de 2023 y 2022.

1.2 Sistemas Operativos

Actualmente tenemos 3 grandes sistemas operativos en el mercado[23]:

- Windows
- Unix
- GNU[24]/Linux

[23] Cuotas de mercado de diferentes sistemas operativos:

https://gs.statcounter.com/os-market-share/desktop/worldwide
https://netmarketshare.com

[24] GNU -es un acrónimo recursivo de «GNU no es UNIX»- es un sistema operativo de Software libre, es decir, respeta la libertad de los usuarios. El sistema operativo GNU consiste en paquetes de GNU además de Software libre publicado por terceras partes con distintas licencias que conforman una distribución.

De los cuales, sus dignos representantes son: Windows, macOS, iOS, Android, Chrome OS y GNU/Linux con todas sus diferentes distribuciones[25]. Y sin temor a equivocarnos aseguramos que Android es la distribución de GNU/Linux más popular e iOS es el más popular de los UNIX.

¿Qué Sistema Operativo Usar? ¿Apple o Microsoft? ¿Windows o Linux? ¿Android o iOS? Son preguntas frecuentes que todos nos hemos hecho alguna vez, y es que elegir un sistema operativo, una computadora o un dispositivo móvil no es tan simple. Al menos no lo era años atrás. En la actualidad las diferencias entre sistemas operativos de escritorio son cada vez menos, hasta el punto que prácticamente cualquier servicio Online es compatible con Windows, Mac y GNU/Linux y las principales firmas de Software crean aplicaciones para las tres plataformas principales, salvo excepciones.

Poco tendremos que decir del sistema operativo de Apple, Mac o iOS, ya que son los sistemas operativos más bonitos y que mejores resultados han dado a todos los usuarios que los han probado. Mac es un sistema pensado para los profesionales de los sectores que necesitan de un equipo de cómputo que sea capaz de todo, como los desarrolladores, programadores, diseñadores, periodistas, fotógrafos, músicos, DJ's y muchos más empleos que se benefician de este sistema operativo.

Después tenemos a Windows, un sistema operativo versátil pensado principalmente para uso doméstico, aunque eso no quita que muchas empresas utilicen Windows en sus equipos de cómputo, ya que es un sistema operativo que puede dar muy buenos resultados en este aspecto.

Sin embargo, llegamos a Linux, el gran desconocido por muchos. Un sistema operativo mucho más versátil que Windows y que puede ser igual

[25] Una distribución de Linux es un sistema operativo compuesto por el Kernel de Linux, herramientas GNU, Software adicional y un administrador de paquetes. También puede incluir un servidor de pantalla y un entorno de escritorio que se utilizarán como sistema operativo de escritorio normal. El término es distribución de Linux (o distribución en forma abreviada) porque una entidad como Debian o Ubuntu 'distribuye' el Kernel de Linux junto con todo el Software y las utilidades consideradas por cada entidad como necesarias (como administrador de red, administrador de paquetes, entornos de escritorio, etc.) para que pueda ser utilizado como sistema operativo. Sus distribuciones también asumen la responsabilidad de proporcionar actualizaciones para mantener el Kernel y otras utilidades.

Entonces, Linux es el Kernel, mientras que la distribución de Linux es el sistema operativo. Esta es la razón por la que también se les conoce como sistemas operativos basados en Linux (hay otros Kernels como son FreeBSD, NetBSD y Hurd).

o más profesional que Mac. Sin embargo, la ventaja que tienen estos dos sistemas operativos, es que vienen ya preparados y configurados para el tipo de mercado al que van dirigidos, pero GNU/Linux no. Esto es una ventaja y una desventaja al mismo tiempo, ya que si tenemos práctica, podemos hacer que el sistema operativo se adapte a nuestras necesidades sin problemas[26], además es Software libre.

1.3 Seguridad TIC

La seguridad TIC (Information Technology Security o IT Security) es un tema de actualidad, ya que cualquier profesional o empresa que use las Tecnologías de la Información y de la Comunicación, debe situarse en la vanguardia de la tecnología.

Pero, ¿qué significa seguridad TIC?, ¿qué es? La seguridad TIC es la responsable de implantar las medidas de seguridad necesarias para procurar la protección de la información a través de diferentes tipos de tecnología.

Así, es capaz de proteger los datos personales y de las empresas, tanto de formatos electrónicos o digitales, como en papel.

Seguramente, más de una vez han oído hablar de la palabra ciberseguridad como si fuera equivalente de seguridad TIC. Pero nada más lejos de

[26]El sistema operativo OpenKylin 2.0 de China presentado en 2024 se destaca por su capacidad para ejecutar tareas de inteligencia artificial de manera local, sin necesidad de conectarse a la nube. Esta característica no solo mejora la velocidad de procesamiento, sino que también protege mejor la privacidad del usuario, ya que no es necesario enviar datos sensibles a servidores externos.

Una de las herramientas más destacadas de este sistema operativo es el "Asistente de IA Kylin", que permite controlar el ordenador mediante la voz, generar imágenes a partir de texto, resumir reuniones y ofrecer herramientas de codificación inteligente para desarrolladores.

Estas funcionalidades están diseñadas para aumentar la productividad y hacer que las tareas diarias sean más fáciles y eficientes. Para los profesionales, esto significa una mayor productividad, ya que el sistema puede gestionar tareas rutinarias y optimizar el flujo de trabajo. Para los usuarios promedio, el sistema ofrece una interfaz más intuitiva y fácil de usar, lo que facilita el acceso a la tecnología.

Aunque las ventajas de un sistema operativo con inteligencia artificial son muchas, también presenta desafíos. La privacidad es una preocupación clave, ya que este tipo de sistemas necesita acceder a los datos del usuario para ofrecer una experiencia personalizada. Los desarrolladores deben asegurarse de implementar medidas de seguridad robustas y políticas de privacidad claras para mantener la confianza de los usuarios (aunque en este caso debemos recordar que se habla de China).

la realidad: la ciberseguridad es un subtipo de la seguridad TIC. De este modo, la ciberseguridad, es la encargada de la protección de los datos de la organización respecto a los posibles ataques que tengan como origen internet.

Pero, de todas formas, la información y todos los datos personales y de las empresas, no sólo se enfrentan a problemas de seguridad en internet, sino que también fuera de él. El modelo de defensa debe abarcar:

- Políticas, procedimientos y concientización
- Seguridad física
- Seguridad de perímetro
- Seguridad de la red
- Seguridad del equipo
- Seguridad de las aplicaciones
- Seguridad de los datos

Amenazas Físicas y sus Repercusiones para la Seguridad TIC Estas, pueden darse por diversos motivos. Así, es posible encontrar las generadas por las radiaciones electromagnéticas debidas a un teclado inalámbrico o el mismo acceso libre a la red Wi-Fi.

Dentro de estas redes Wi-Fi están los Sniffers, que no son más que sistemas que, por decirlo de alguna manera, recopilan cualquier dato que encuentren de los usuarios. Por lo tanto, son ideales para realizar auditorías en las propias redes, para corroborar y verificar el tráfico de una organización y además, monitorizar el comportamiento que tiene dentro de la propia red y sus movimientos.

No obstante, si un Hacker encuentra un acceso, con los Sniffer, podría apoderarse de todos los datos del usuario y contraseñas, por lo que el sistema no es demasiado adecuado ni fiable. Es por ello, que no es recomendable utilizar este sistema en las empresas, ya que puede suponer un grave problema para la seguridad de la información que se esté gestionando de esta manera.

Es usual encontrarse Sniffers, por ejemplo, en las universidades, con objeto de evitar que se conecten a la red Wi-Fi personas que no sean del propio centro y dañen el sistema.

Otra de las amenazas físicas que podemos encontrar y que en realidad, no puede evitarse, es la debida a los accidentes naturales. Como es evidente, se trata de que tenga lugar un accidente natural en el lugar donde se encuentre el Hardware, de manera que se dañe a consecuencia de un incendio, humedad, apagones, etc.

Amenazas Lógicas Este tipo de amenazas, son programas que han sido diseñados explícitamente para dañar el sistema. Básicamente, se aprovechan de cualquier vulnerabilidad, fallo o debilidad que exista en un sistema, para poder atacarlo y, finalmente, acceder a él.

Así, se pueden encontrar dos tipos:

- Intencionados: se trata de programas que tienen como objetivo hacer daño, como por ejemplo los Malware o Software malicioso, los Spyware, Jokes, Virus, Backdoors, Dialers, etc. entre otros.
- No intencionados: este tipo, tiene lugar cuando un programador comete alguna clase de error o fallo en la programación, dando lugar, por ejemplo a Bugs o Exploits.

Amenazas del propio usuario este punto es el más sensible. Normalmente, en cualquier empresa, los empleados, o usuarios en sí son los eslabones más débiles en lo que respecta a la seguridad TIC.

Esto es, cualquier usuario de una empresa trabaja con datos, independientemente del permiso que tenga para gestionarlos, editarlos o verificarlos, pues se trata de una cadena. Así, encontramos usuarios que, por diversos motivos, son la fuente de los principales fallos de seguridad TIC que tienen lugar en una empresa, y son a los que se les suele denominar eslabones débiles.

Entonces, es fundamental que sepan la forma en la que hay que proceder, con objeto de poder evitar cualquier tratamiento erróneo de los datos.

Este tipo de usuarios suele actuar de dos formas:

- Activa: aquí, el usuario causa daño de manera consciente, bien sea por dañar o por sustraer información o datos específicos de la empresa. Como ejemplos, tenemos a los Hackers, antiguos empleados o piratas informáticos.
- Pasiva: cuando daña al sistema sin intención de hacerlo, por falta de formación, conocimiento o por querer acceder a una información a la

que no tiene acceso. Por ello, es preciso establecer niveles de permiso para los accesos a los sistemas de gestión documental.

1.4 Formación en Seguridad de la Información

Finalmente, los cursos de formación respecto a la seguridad de la información se tornan fundamentales para poder manejarse y recordar cualquier norma que sea imprescindible. Por ejemplo, la gestión segura de las contraseñas, del correo electrónico, la gestión de la documentación, etc.

Pero, de todas formas, la información y todos los datos personales y de las empresas, no sólo se enfrentan a problemas de seguridad en internet, sino que también fuera de él. Algunas de estas amenazas, son las que van a desarrollarse en este capítulo, pero si quiere conocer la norma ISO por excelencia para procurar la seguridad de la información en las empresas, le recomendamos que visite por ejemplo la página sobre la norma ISO 27001 o Cybersecurity Framework.

En el presente texto describiremos los principios de la seguridad, privacidad y vigilancia de la información en nuestros dispositivos de cómputo como en la red, que es más un problema de protección de datos, y debe estar básicamente orientada a asegurar la propiedad intelectual y la información importante de las organizaciones y de las personas. Los riesgos de la información están presentes cuando coinciden fundamentalmente dos elementos: las amenazas de ataques, y las vulnerabilidades de la tecnología; conceptos íntimamente relacionados donde no es posible ninguna consecuencia sin la presencia conjunta de estos.

Además daremos algunas recomendaciones de ciberseguridad más apremiantes para entre otras cosas: generar contraseñas robustas, mantener la seguridad de los sistemas operativos en nuestros dispositivos, promover una navegación segura, así como el uso seguro de las herramientas en la nube, además de algunas pautas para proteger dispositivos móviles y el uso seguro de redes sociales, entre otras.

Pero debemos tener presente que el primero de enero del 2018 se dio a conocer al público, que 6 meses antes se habían detectado dos distintos fallos en los procesadores de los equipos de cómputo, comunicaciones y redes de internet que usamos. Esto para dar tiempo a los desarrolladores de procesadores y de sistemas operativos de implementar estrategias para mitigar el problema. Estos son problemas de diseño de los procesadores de Intel, AMD, IBM POWER y ARM, esto significa que procesos con privilegios bajos (aque-

llos que lanzan las aplicaciones de usuario convencionales) podían acceder a la memoria del Kernel del sistema operativo.

Ese primer problema, es en realidad solo parte del desastre. Los datos de dichos fallos provienen principalmente de un grupo de investigadores de seguridad formados por expertos del llamado Project Zero[27] de Google. Ellos han publicado los detalles de dos ataques (no son los únicos) basados en estos fallos de diseño. Los nombres de esos ataques son Meltdown y Spectre. Y en un sitio Web dedicado a describir estas vulnerabilidades destacan que "aunque los programas normalmente no tienen permiso para leer datos de otros programas, un programa malicioso podría explotar Meltdown y/o Spectre y apropiarse de secretos almacenados en la memoria de otros programas".

Como revelan en su estudio, la diferencia fundamental entre ambos es que Meltdown permite acceder a la memoria del sistema, mientras que Spectre permite acceder a la memoria de otras aplicaciones para robar esos datos y como esto es un problema de Hardware, todos los sistemas operativos que trabajan en dichos procesadores están expuestos y han estado trabajando para tratar de mitigar el problema.

Por otro lado, para muchos usuarios, Linux y Mac OS son dos sistemas operativos más seguros que Windows de Microsoft, pero con todo, hay algunas distribuciones especializadas de Linux que satisfacen las necesidades de temas relacionados con la seguridad, pruebas de penetración, análisis forense y auditorías de seguridad.

Las distribuciones seguras intentan preservar la privacidad y el anonimato, ayudan a utilizar internet de forma anónima y evitar la censura en prácticamente cualquier lugar y cualquier equipo de cómputo, pero sin dejar rastro a menos que lo solicite explícitamente.

Las distribuciones para pruebas de penetración ofrecen herramientas para penetración, análisis forense y auditorías de seguridad en donde se realizan distintos tipos de tareas que identifican, en una infraestructura objetivo, las vulnerabilidades que podrían explotarse y los daños que podría causar un atacante. En otras palabras, se realiza un proceso de Hacking ético para identificar qué incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de tal forma que se eviten estos ataques.

Las distribuciones anónimas ofrecen niveles adicionales de privacidad y seguridad y se complementan con las distribuciones para pruebas de pe-

[27] https://googleprojectzero.blogspot.com/

netración que ofrecen herramientas para penetración y auditorías de seguridad (mediante el uso de tecnologías como TOR, Sandbox, Firewall, herramientas criptográficas, etc.). De ambos tipos de Software hay varias alternativas diferentes, tanto comerciales como de Software libre, por lo que decidirse por una u otra, en ocasiones puede ser una tarea un tanto complicada. Es por ello que aquí listamos algunas de las distribuciones de Linux más usadas en la actualidad, apartados con los que cada vez debemos prestar más atención.

Existe una cita de Sun Tzu (General, estratega militar y filósofo de la antigua China) que dice: «Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cientos de batallas. Si te conoces a ti mismo, pero no al enemigo, por cada victoria que ganes también sufrirás una derrota. Si no conoces ni al enemigo ni a ti mismo, sucumbirás en cada batalla.»

De dicha frase podemos concluir que, el conocimiento de nuestras debilidades y las debilidades de nuestros adversarios, nos llevará de una forma segura hacia la victoria o derrota. Y extrapolando esto a la Informática, GNU/Linux, los actuales grupos de Hackers y los ataques informáticos, nos queda más que claro, que debemos conocer a detalle tanto nuestros Sistemas Operativos libres y abiertos como las vulnerabilidades que pueden ser explotadas por terceros, para así mitigar los riesgos de dichos ataques.

1.5 ¿Qué tan Seguro es Linux/Unix?

No es ningún secreto que el sistema operativo que elijas es un determinante clave de su seguridad (no sólo en internet, también la privacidad de tus datos en el equipo que usas). Después de todo, el sistema operativo es el Software más crítico que se ejecuta en nuestra computadora o dispositivo inteligente: administra su memoria y procesos, así como todo su Software y Hardware. El consenso general entre los expertos es que Linux/Unix es un sistema operativo altamente seguro, posiblemente el sistema operativo más seguro por diseño. Examinaremos aquí algunos factores clave que contribuyen a la sólida seguridad de Linux/Unix y veremos el nivel de protección contra vulnerabilidades y ataques que Linux ofrece a los administradores y usuarios.

Seguro por Diseño Cuando se trata de seguridad, los usuarios de Linux/Unix tienen una clara ventaja sobre sus contrapartes que usan Windows o MacOs. A diferencia de los sistemas operativos propietarios, Linux/Unix, en

muchos sentidos, tiene seguridad integrada en su diseño central. El sistema operativo de código abierto cada vez más popular es de alta flexibilidad, configurable y diverso. También implementa un modelo estricto de privilegios de usuario y ofrece una selección de defensas de seguridad de Kernel integradas para protegerse contra vulnerabilidades y ataques. La transparencia del código fuente de Linux/Unix significa que las vulnerabilidades en él, que son inevitables hasta cierto punto en cualquier sistema operativo, casi siempre son de corta duración. Echemos un vistazo más de cerca a cada uno de estos factores y cómo contribuye a la seguridad anunciada de Linux/Unix.

La Ventaja de la Seguridad de Código Abierto El código fuente de Linux/Unix se somete a una revisión exhaustiva y constante por parte de los miembros de la vibrante comunidad global de código abierto y, como resultado de este escrutinio, las vulnerabilidades de seguridad de Linux/Unix generalmente se identifican y eliminan muy rápidamente. Por el contrario, los proveedores propietarios como Microsoft y Apple emplean un método conocido como "seguridad por oscuridad", donde el código fuente se oculta a los extraños en un intento de ocultar las vulnerabilidades de los actores de amenazas. Sin embargo, este enfoque generalmente es ineficaz para prevenir las vulnerabilidades modernas y, en realidad, socava la seguridad del código fuente "oculto" al evitar que personas ajenas identifiquen y reporten fallas antes de que sean descubiertas por actores malintencionados. Seamos realistas: cuando se trata de descubrir errores de seguridad, un pequeño equipo de desarrolladores propietarios no es rival para la comunidad mundial de usuarios-desarrolladores de Linux/Unix que están profundamente involucrados en su trabajo tanto para su propio beneficio como para el beneficio de la comunidad.

Un Modelo Superior de Privilegios de Usuario A diferencia de Windows, donde "todo el mundo es administrador", Linux/Unix restringe en gran medida el acceso a la raíz a través de un modelo estricto de privilegios de usuario. En Linux/Unix, el superusuario posee todos los privilegios, y a los usuarios comunes solo se les otorgan suficientes permisos para realizar tareas comunes. Debido a que los usuarios de Linux/Unix tienen pocos derechos de acceso automático y requieren permisos adicionales para abrir archivos adjuntos, acceder a archivos o ajustar las opciones del Kernel, es más difícil propagar Malware y Rootkits en un sistema Linux/Unix. Por lo tanto, estas

restricciones inherentes sirven como una defensa clave contra los ataques y el compromiso del sistema.

Defensas de Seguridad de Kernel Incorporadas El Kernel de Linux cuenta con una variedad de defensas de seguridad integradas que incluyen Firewalls que utilizan filtros de paquetes en el Kernel, el mecanismo de verificación de Firmware UEFI Secure Boot, la opción de configuración Linux Kernel Lockdown y los sistemas de mejora de seguridad SELinux o AppArmor Mandatory Access Control (MAC). . Al habilitar estas funciones y configurarlas para brindar el más alto nivel de seguridad en una práctica conocida como autoprotección del Kernel de Linux, los administradores pueden agregar una capa adicional de seguridad a sus sistemas.

Seguridad a Través de la Diversidad Existe un alto nivel de diversidad posible dentro de los entornos de Linux/Unix como resultado de las muchas distribuciones de Linux/Unix disponibles y las diferentes arquitecturas de sistema y componentes que presentan. Esta diversidad no solo ayuda a satisfacer los requisitos individuales de los usuarios, sino que también ayuda a protegerse contra los ataques al dificultar que los actores maliciosos elaboren de manera eficiente Exploits que puedan usarse contra una amplia gama de sistemas Linux/Linux. Por el contrario, la "monocultura" homogénea de Windows convierte a Windows en un objetivo de ataque relativamente fácil y eficiente (algo parecido también les pasa a las Mac).

Además de la diversidad de diseño que se ve en Linux/Unix, ciertas distribuciones seguras de Linux/Unix se diferencian en formas que abordan específicamente las preocupaciones de seguridad y privacidad avanzadas compartidas entre los Pentesters, los ingenieros inversos y los investigadores de seguridad.

Altamente Flexible y Configurable Hay muchas más opciones de configuración y control disponibles para los administradores de Linux/Unix que para los usuarios de Windows y MacOs, muchas de las cuales se pueden usar para mejorar la seguridad. Por ejemplo, los administradores de sistemas de Linux tienen la capacidad de usar SELinux o AppArmor para bloquear su sistema con políticas de seguridad que ofrecen controles de acceso granulares, proporcionando una capa adicional crítica de seguridad en todo el sistema. Los administradores también pueden usar la opción de configuración Linux

Kernel Lockdown para fortalecer la división entre los procesos de la zona de usuario y el código del Kernel, y pueden fortalecer el archivo sysctl.conf, el principal punto de configuración de parámetros del Kernel para un sistema Linux, para darle a su sistema una base más segura.

Linux/Unix: Un Objetivo Cada Vez Más Popular Entre los Ciber Delincuentes Linux/Unix alimenta la mayoría de los dispositivos y supercomputadoras de alto valor del mundo y la base de usuarios del sistema operativo está creciendo constantemente, y los ciberdelincuentes han tomado nota de estas tendencias. Los autores y operadores de Malware apuntan cada vez más a los sistemas Linux/Unix en sus campañas maliciosas. Por ejemplo, en los últimos años han estado plagados de cepas emergentes de Malware para Linux: Cloud Snooper, EvilGnome, HiddenWasp, QNAPCrypt, GonnaCry, FBOT y Tycoon se encuentran entre las más notorias. Dicho esto, Linux sigue siendo un objetivo relativamente pequeño, con el 96 % del nuevo Malware dirigido a Windows en 2022. Además, el reciente aumento de los ataques de Malware de Linux no es un reflejo de la seguridad de Linux. La mayoría de los ataques a los sistemas Linux se pueden atribuir a configuraciones incorrectas y una administración deficiente, lo que destaca una falla generalizada entre los administradores de sistemas Linux para priorizar la seguridad.

Afortunadamente, a medida que el Malware de Linux/Unix continúa siendo cada vez más frecuente y problemático, Linux/Unix cuenta con protección integrada contra ataques de Malware a través de su estricto modelo de privilegios de usuario y diversidad de diseño, y hay una selección de excelentes herramientas, Kits de herramientas y utilidades de análisis de Malware e ingeniería inversa que incluyen REMnux, Chkrootkit, Rkhunter, Lynis y Linux Malware Detect (LMD) disponibles para ayudar a los administradores a detectar y analizar Malware en sus sistemas.

Para Tomar en Cuenta La seguridad del sistema operativo que implementa es un determinante clave de su seguridad en internet, pero de ninguna manera es una protección segura contra Malware, Rootkits y otros ataques. La seguridad efectiva depende de la defensa en profundidad, y otros factores, incluida la implementación de las mejores prácticas de seguridad y el comportamiento inteligente internet, juegan un papel central en su postura de seguridad digital. Dicho esto, elegir un sistema operativo seguro es de suma importancia, ya que el sistema operativo es la pieza de Software más crítica

que se ejecuta en nuestros dispositivos computacionales, y Linux es una excelente opción ya que tiene el potencial de ser altamente seguro, posiblemente más que su contraparte propietaria, debido a su código de fuente abierta, modelo estricto de privilegios de usuario, diversidad y base de usuarios relativamente pequeña.

Sin embargo, Linux/Unix no es una "bala de plata" cuando se trata de seguridad digital: el sistema operativo debe configurarse de manera adecuada y segura, y los administradores de sistemas deben practicar una administración responsable y segura para evitar ataques. Además, es fundamental tener en cuenta que la seguridad tiene que ver con las compensaciones, tanto entre seguridad y facilidad de uso como entre seguridad y facilidad de uso. Los administradores deben configurar sus sistemas para que sean tan seguros como sea práctico dentro de su entorno. En lo que respecta a la conveniencia, Linux tiene una pequeña curva de aprendizaje, pero ofrece importantes ventajas de seguridad sobre Windows o MacOs.

1.6 Agradecimientos

Este texto es una recopilación de múltiples fuentes, nuestra aportación -si es que podemos llamarla así- es plasmarlo en este documento, en el que tratamos de dar coherencia a nuestra visión de los temas desarrollados.

En la realización de este texto se han revisado -en la mayoría de los casos indicamos la referencia, pero pudimos omitir varias de ellas, por lo cual pedimos una disculpa- múltiples páginas Web, artículos técnicos, libros, entre otros materiales bibliográficos, los más representativos y de libre acceso los ponemos a su disposición en la siguiente liga:

Herramientas
http://132.248.181.216/Herramientas/

Además, la documentación y los diferentes ejemplos que se presentan en este trabajo, se encuentran disponibles en dicha liga, para que puedan ser copiados desde el navegador y ser usados. En aras de que el interesado pueda correr dichos ejemplos y afianzar sus conocimientos, además de que puedan ser usados en diferentes ámbitos a los presentados aquí.

Este proyecto fue posible gracias al apoyo recibido por la Facultad de Ciencias de la Universidad Nacional Autónoma de México (UNAM) y al

tiempo robado a nuestras actividades académicas, principalmente durante el período de confinamiento de los años 2020 a 2022.

2 Sistemas Operativos

Actualmente tenemos 3 grandes sistemas operativos en el mercado[28]:

- Windows
- Unix
- GNU[29]/Linux

De los cuales, sus dignos representantes son: Windows, macOS, iOS, Android, Chrome OS y GNU/Linux con todas sus diferentes distribuciones[30]. Y sin temor a equivocarnos aseguramos que Android es la distribución de GNU/Linux más popular e iOS es el más popular de los UNIX.

¿Qué es un Sistema Operativo? El conjunto de programas informáticos que permiten la administración eficaz de los recursos de una computadora es conocido como sistema operativo o Software de sistema. Estos programas comienzan a trabajar apenas se enciende el equipo, ya que gestionan el Hardware desde los niveles más básicos y permiten además la interacción

[28] Cuotas de mercado de diferentes sistemas operativos:

https://gs.statcounter.com/os-market-share/desktop/worldwide
https://netmarketshare.com

[29] GNU -es un acrónimo recursivo de «GNU no es UNIX»- es un sistema operativo de Software libre, es decir, respeta la libertad de los usuarios. El sistema operativo GNU consiste en paquetes de GNU además de Software libre publicado por terceras partes con distintas licencias que conforman una distribución.

[30] Una distribución de Linux es un sistema operativo compuesto por el Kernel de Linux, herramientas GNU, Software adicional y un administrador de paquetes. También puede incluir un servidor de pantalla y un entorno de escritorio que se utilizarán como sistema operativo de escritorio normal. El término es distribución de Linux (o distribución en forma abreviada) porque una entidad como Debian o Ubuntu 'distribuye' el Kernel de Linux junto con todo el Software y las utilidades consideradas por cada entidad como necesarias (como administrador de red, administrador de paquetes, entornos de escritorio, etc.) para que pueda ser utilizado como sistema operativo. Sus distribuciones también asumen la responsabilidad de proporcionar actualizaciones para mantener el Kernel y otras utilidades.

Entonces, Linux es el Kernel, mientras que la distribución de Linux es el sistema operativo. Esta es la razón por la que también se les conoce como sistemas operativos basados en Linux (hay otros Kernels como son FreeBSD, NetBSD y Hurd).

con el usuario. Cabe destacar que los sistemas operativos no funcionan sólo en las computadoras. Por el contrario, este tipo de sistemas se encuentran en la mayoría de los dispositivos electrónicos que utilizan microprocesadores: el Software de sistema posibilita que el dispositivo cumpla con sus funciones -por ejemplo, un teléfono móvil o un reproductor de DVD-.

El sistema operativo cumple con cinco funciones básicas:

- Proporciona la interfaz del usuario -gráfica o de texto-
- La administración de recursos
- La administración de archivos
- La administración de tareas
- El servicio de soporte y utilidades

En cuanto a la interfaz del usuario, el sistema se encarga de que el usuario pueda ejecutar programas, acceder a archivos y realizar otras tareas con la computadora. La administración de recursos permite el control del Hardware, incluyendo los periféricos y la red. El Software de sistema también se encarga de la gestión de archivos, al controlar la creación, la eliminación y el acceso a los mismos, así también, de la administración de las tareas informáticas que ejecutan los usuarios finales. Por último, podemos mencionar que el servicio de soporte se encarga de actualizar las versiones, mejorar la seguridad del sistema, agregar nuevas utilidades, controlar los nuevos periféricos que se agregan a la computadora y corregir los errores del Software.

Tipos de Sistemas Operativos en Función de la Administración de las Tareas Podemos distinguir dos clases de sistemas operativos en función de cómo administran sus tareas, pueden ser:

Sistemas Operativos Monotarea: son sistemas operativos que únicamente cuentan con la capacidad para realizar una tarea al mismo tiempo. Son los sistemas más antiguos, que también llevan aparejados un CPU de menor capacidad. En estos casos, si el equipo está imprimiendo, no atenderá a las nuevas órdenes, ni será capaz de iniciar un nuevo proceso hasta que el anterior haya finalizado.

Sistemas Operativos Multitarea: son los sistemas operativos más modernos, con capacidad para el procesamiento de varias tareas al mismo tiempo. Cuentan con la capacidad para ejecutar varios procesos en uno o más procesadores, por lo que existe la posibilidad de que sean utilizados por varios usuarios al mismo tiempo, y podrían aceptar múltiples conexiones a través de sesiones remotas.

Tipos de Sistemas Operativos en Función de la Administración de los Usuarios También es posible realizar una división de los sistemas operativos en función de la forma en la que se administran los usuarios, como vemos a continuación:

Sistema de Administración Monousuario: sólo pueden gestionar un usuario al mismo tiempo. Así, a pesar de que varios usuarios pueden tener acceso al sistema, solo un usuario puede acceder para realizar y ejecutar operaciones y programas.

Sistemas de Administración Multiusuario: se refiere a todos aquellos sistemas operativos que permiten el empleo de sus procesamientos y servicios al mismo tiempo. Así, el sistema operativo cuenta con la capacidad de satisfacer las necesidades de varios usuarios al mismo tiempo, siendo capaz de gestionar y compartir sus recursos en función del número de usuarios que estén conectados a la vez.

¿Qué Sistema Operativo Usar? ¿Mac o Microsoft? ¿Windows o Linux? ¿Android o iOS? Son preguntas frecuentes que todos nos hemos hecho alguna vez, y es que elegir un sistema operativo, una computadora o un dispositivo móvil no es tan simple. O al menos no lo era años atrás. En la actualidad las diferencias entre sistemas operativos de escritorio son cada vez menos, hasta el punto que prácticamente cualquier servicio Online es compatible con Windows, Mac y GNU/Linux y las principales firmas de Software crean aplicaciones para las tres plataformas principales, salvo excepciones. Lo mismo empieza a ocurrir con el Hardware.

Poco tendremos que decir del sistema operativo de Apple, Mac o iOS (ambos son derivados de Darwin BSD que es un sistema operativo tipo UNIX), ya que son los sistemas operativos más bonitos y que mejores resultados han dado a todos los usuarios que los han probado. Mac es un sistema pensado

para los profesionales de los sectores que necesitan de un equipo de cómputo que sea capaz de todo, como los desarrolladores, programadores, diseñadores, periodistas, fotógrafos, músicos, DJ's y muchos más empleos que se benefician de este sistema operativo.

Después tenemos a Windows, un sistema operativo versátil pensado sobre todo para un uso doméstico, aunque eso no quita que muchas empresas utilicen Windows en sus equipos de cómputo ya que es un sistema operativo que puede dar muy buenos resultados en este aspecto.

Sin embargo, llegamos a Linux, el gran desconocido por muchos. Un sistema operativo mucho más versátil que Windows y que puede ser igual o más profesional que Mac. Sin embargo, la ventaja que tienen estos dos sistemas operativos, es que vienen ya preparados y configurados para el tipo de mercado al que van dirigidos, pero GNU/Linux no.

Esto es una ventaja y una desventaja al mismo tiempo, ya que si tenemos práctica, podemos hacer que el sistema operativo se adapte a nuestras necesidades sin problemas, pero si no tienes práctica, puede que sea demasiado lo que tienes que configurar.

Cuota de Mercado para los Sistemas Operativos Febrero y Agosto son los meses en los que miles de compañías analizan el tráfico que les llega de usuarios a sus páginas Web y desde que plataformas llegan, según un informe de International Data Corporation (https://www.idc.com), Statcounter (https://www.statcounter.com) y The Linux Foundation (https://www.linux-fundation.org) en el último año tenemos:

- En el segmento de los sistemas operativos de escritorio basados en Linux ha subido su cuota de mercado llegando al 4%, esto no parecerá mucho, pero si nos fijamos bien, vemos que Mac tiene un 15% -basado en Unix-, Chrome OS -usa el Kernel de Linux- tiene 2% y Windows el resto.

- En el segmento de teléfonos inteligentes (SmartPhones) y tabletas basadas en Android -usa el Kernel de Linux- tiene 77 %, iOS tiene 19 % -basado en Unix- y 4% HarmonyOS de Huawei -que usa una variante del Kernel de Linux-.

- En el segmento de servidores se estima que más del 60% de los servidores a nivel mundial usan Linux, 1% usan Unix y el resto Windows. Pero en los principales servidores del mundo (un millón) 96 % usan Linux.

- El 90% de toda la infraestructura Cloud corre usando Linux. Es de destacar que en el servicio de servidores Microsoft Azure, el sistema predominante es Linux.
- En el segmento de supercomputadoras, Linux tiene la cuota más importante del mercado; es utilizado en los Top 500 sistemas de supercómputo de alto desempeño del mundo[31].

Hay que decir, que hoy en día y tal y como están las cosas, no existe un sistema operativo que sea definitivo. Así que la pregunta de si GNU/Linux[32] es mejor que Windows o Mac no tiene sentido, ya que cada sistema operativo tiene sus pros y sus contras.

Pero la disyuntiva sigue ahí. ¿Debemos usar Windows en nuestro equipo de cómputo?, ¿nos conviene pasarnos a Linux?. Hay razones a favor y en contra para todos los gustos.

Número de Líneas del Código Fuente de un Sistema Operativo
Pese a que existen múltiples variantes de cada sistema operativo, se han dado a conocer los números de líneas de código fuente que componen la vertiente más usada de algunos sistemas operativos:

- Microsoft Windows 3.1 (Abril de 1992): 3 millones de líneas ($200 USD en 1992)
- Microsoft Windows 95 (Agosto de 1995): 15 millones de líneas (Home $109.95 y Pro$ 209.95 USD en 1995)
- Microsoft Windows NT 4.0 (Julio 1996): 12 millones de líneas (5 usuarios $809, 10 usuarios $1,129 USD en 1996)

[31] Existe el Ranking de las 500 supercomputadoras más poderosas del mundo (esta se actualiza cada seis meses en junio y noviembre) y puede ser consultada en:
https://top500.org
La cuota de supercomputadoras con GNU/Linux ha sido de: 2012 (94%), 2013 (95%), 2014 (97%), 2015 (97.2%), 2016 (99.6%), 2017 (99.6%), 2018 (100%), 2019 (100%), 2020 (100%).

[32] Los resultados de GNU/Linux son muy satisfactorios para los desarrolladores y partícipes de la comunidad Linux, pero todavía hace falta mucho por hacer para que tenga una cuota significativa en el escritorio y esto sólo será posible si los distribuidores de equipo generan un esquema más agresivo para vender máquinas con Linux preinstalado.

- Microsoft Windows 2000 (Febrero 2000): 29 millones de líneas (Pro $319 USD en 2000)
- Microsoft Windows XP (Octubre 2001): 45 millones de líneas (Home $175 US y Pro $ 255 USD en 2001)
- Microsoft Windows Vista (Enero 2007): 50 millones de líneas (Home Premium $239.99 USD en 2007)
- Microsoft Windows 7 (Octubre 2009): 40 millones de líneas (Home Premium $199.99 USD en 2009)
- Microsoft Windows 8 (Octubre 2012): 60 millones de líneas (Home $119.99 US y Pro $ 199.99 USD en 2013)
- Microsoft Windows 10 (Julio 2015): 60 millones de líneas sin Cortana y 65 millones de líneas con Cortana ($139.99 USD en 2019)
- Sun Solaris (Octubre de 1998) 7.5 millones de líneas
- Red Hat Linux 6.2 (Marzo de 2000): 17 millones de líneas
- Red Hat Linux 7.1 (Abril de 2001): 30 millones líneas
- Red Hat Linux 8.0 (Septiembre de 2002): 50 millones de líneas
- Fedora Core 4 (Mayo de 2005): 76 millones de líneas
- Fedora 9 (Mayo del 2008): 205 millones de líneas
- Debian GNU/Linux 3.0 "Woody" (Julio de 2002): 105,000,000 líneas
- Debian GNU/Linux 3.1 "Sarge" (Junio de 2005); 229,500,000 líneas
- Debian GNU/Linux 7 "Wheezy" (Mayo 2013): 419 millones de líneas
- Debian GNU/Linux 10 "Buster" (Julio 2019): 1,077,110,982 líneas
- Debian GNU/Linux 11 "Bullseye" (Agosto 2021): 1,152,960,944 líneas
- Debian GNU/Linux 12 "bookworm" (Junio 2023): 1,341,564,204 líneas
- Kernel Linux 0.01 (Septiembre 1991): 8,413 líneas

- Kernel Linux 1.0 (Marzo 1994): 176,250 líneas
- Kernel Linux 2.6 (Diciembre 2003): 5,475,685 líneas
- Kernel Linux 4.12 (Julio 2017): 24 millones líneas
- Kernel Linux 5.14 (Julio 2021): 29.7 millones de líneas
- Kernel Linux 6.13 (Enero 2025): 40 millones de líneas

El Kernel o Núcleo Es un componente fundamental de cualquier sistema operativo. Es el encargado de que el Software y el Hardware de cualquier equipo de cómputo puedan trabajar juntos en un mismo sistema, para lo cual administra la memoria de los programas y procesos ejecutados, el tiempo de procesador que utilizan los programas, o se encarga de permitir el acceso y el correcto funcionamiento de periféricos y otros elementos físicos del equipo.

Kernel de Linux el núcleo del sistema operativo Linux/Unix (llamado Kernel) es un programa escrito casi en su totalidad en lenguaje C, con excepción de una parte del manejo de interrupciones, expresada en el lenguaje ensamblador del procesador en el que opera, el Kernel reside permanentemente en memoria y alguna parte de él está ejecutándose en todo momento. Pero es muy común confundir al Kernel de Linux con una distribución como Debian y Ubuntu, Linux solo es un núcleo (hay otros como son FreeBSD, NetBSD y Hurd).

Durante mucho tiempo el núcleo Linux solo funcionaba en la serie de máquinas x86 de Intel, desde el 386 en adelante. Sin embargo, hoy día esto ya no es cierto. El núcleo Linux se ha adaptado a una larga y creciente lista de arquitecturas. Siguiendo esos pasos, la distribución Debian GNU/Linux se ha adaptado a estas plataformas. En general este proceso tiene un comienzo difícil (hay que conseguir que la *libc* y el enlazador dinámico funcionen sin trabas), luego sigue un trabajo relativamente largo y rutinario, de conseguir recompilar todos los paquetes bajo las nuevas arquitecturas.

Debian GNU/Linux es un sistema operativo, no un núcleo (en realidad es más que un SO, ya que incluye miles de aplicaciones). Para probar esta afirmación, aun cuando la mayor parte de adaptaciones se hacen sobre núcleos Linux, también existen adaptaciones basadas en los núcleos FreeBSD, NetBSD y Hurd.

Linux es multiprogramado, dispone de memoria virtual, gestión de memoria, conectividad en red y permite bibliotecas compartidas. Linux es multiplataforma y es portable a cualquier arquitectura siempre y cuando está disponga de una versión de GCC compatible.

La parte de un sistema operativo que se ejecuta sin privilegios o en espacio de usuario es la biblioteca del lenguaje C, que provee el entorno de tiempo de ejecución, y una serie de programas o herramientas que permiten la administración y uso del núcleo y proveer servicios al resto de programas en espacio de usuario, formando junto con el núcleo el sistema operativo.

En un sistema con núcleo monolítico como Linux la biblioteca de lenguaje C (*libc*) consiste en una abstracción de acceso al núcleo. Algunas bibliotecas como la biblioteca de GNU proveen funcionalidad adicional para facilitar la vida del programador y usuario o mejorar el rendimiento de los programas. En un sistema con micronúcleo la biblioteca de lenguaje C puede gestionar sistemas de archivos o controladores además del acceso al núcleo del sistema.

A los sistemas operativos que llevan Linux se les llama de forma genérica distribuciones Linux. Estas consisten en una recopilación de software que incluye el núcleo Linux y el resto de programas necesarios para completar un sistema operativo. Las distribuciones más comunes son de hecho distribuciones GNU/Linux o distribuciones Android. El hecho de que compartan núcleo no significa que sean compatibles entre sí. Una aplicación hecha para GNU/Linux no es compatible con Android sin la labor adicional necesaria para que sea multiplataforma.

Las distribuciones GNU/Linux usan Linux como núcleo junto con el entorno de tiempo de ejecución del Proyecto GNU y una serie de programas y herramientas del mismo que garantizan un sistema funcional mínimo. La mayoría de distribuciones GNU/Linux incluye software adicional como entornos gráficos o navegadores Web así como los programas necesarios para permitirse instalar a sí mismas. Los programas de instalación son aportados por el desarrollador de la distribución. Se les conoce como gestores de paquetes. Los creadores de una distribución también se pueden encargar de añadir configuraciones iniciales de los distintos programas incluidos en la distribución.

Las distribuciones Android incluyen el núcleo Linux junto con el entorno de ejecución y herramientas del proyecto AOSP de Google. Cada fabricante de teléfonos dispone de su propia distribución de Android a la cual modifica, elimina o añade programas extra: interfaces gráficas, tiendas de aplicaciones y clientes de correo electrónico son algunos ejemplos de programas suscepti-

bles de ser añadidos, modificados o eliminados. Además de las distribuciones de los fabricantes de teléfonos existen grupos de programadores independientes que también desarrollan distribuciones de Android. LineageOS y Replicant son dos ejemplos de distribuciones Android independientes.

Los usuarios de Linux/Unix estamos acostumbrados a hablar y oír hablar sobre su Kernel[33], el cual puede actualizarse y manipularse en cualquier distribución. Sin embargo, en un sistema operativo tan centrado en el usuario y la sencillez como Windows, su Kernel es un gran desconocido.

Kernel de Windows en la década de los noventa Microsoft estaba basando sus sistemas operativos en los Kernel Windows 9x, donde el código básico tenía muchas similitudes con MS-DOS. De hecho necesitaba recurrir a él para poder operar. Paralelamente, Microsoft también estaba desarrollando otra versión de su sistema dirigido a los servidores llamada Windows NT.

Ambas versiones de Windows fueron desarrollándose por separado. Windows NT era más bien una jugada a largo plazo, una tecnología para ir desarrollando para los Windows del mañana, y en el año 2000 dieron un nuevo paso en esa dirección. A la versión 5.0 de NT la llamaron Windows 2000, y se convirtió en un interesante participante en el sector empresarial.

Tras ver la buena acogida que tuvo, Microsoft decidió llevar NT al resto de usuarios para que ambas ramificaciones convergien. Lo hicieron en octubre del 2001 con la versión 5.1 de Windows NT, que llegó al mercado con el nombre de Windows XP. Por lo tanto, esta versión marcó un antes y un después no sólo por su gran impacto en el mercado, sino porque era el principio de la aventura del Kernel Windows NT en el mundo de los usuarios comunes.

Desde ese día, todas las versiones de Windows han estado basadas en este Kernel con más de 20 años de edad. La versión 5.1.2600 fue Windows XP, la 6.0.6002 fue Windows Vista, y la 6.1.7601 Windows 7. Antes hubo otros

[33] En el caso de los sistemas derivados de Unix y Linux el Kernel lo podemos encontrar en el directorio /boot/, este directorio incluye todos los ejecutables y archivos que son necesarios en el proceso de arranque del sistema y deben ser utilizados antes que el Kernel empiece a dar las órdenes de ejecución de los diferentes módulos del sistema, aquí también es donde reside el gestor de arranque.

En algunas distribuciones al usar un gestor de volúmenes lógico (Logical Volume Manager, LVM) se genera un esquema de particiones con el directorio boot en una partición aparte.

Windows Server 2008 y 2003, y después llegaron las versiones de NT 6.2.9200 llamada Windows 8, la 6.3.9600 o Windows 8, la NT 10.0, también conocida como Windows 10 y finalmente Windows 11.

La principal característica del Kernel de Windows NT es que es bastante modular, y está basada en dos capas principales, la de usuario y la de Kernel. El sistema utiliza cada una para diferentes tipos de programa. Por ejemplo, las aplicaciones se ejecutan en el modo usuario, y los componentes principales del sistema operativo en el modo Kernel. Mientras, la mayoría de los Drivers suelen usar el modo Kernel, aunque con excepciones.

Es por eso que se refieren a él como Kernel híbrido, pero sobre todo también porque permite tener subsistemas en el espacio del usuario que se comunicaban con el Kernel a través de un mecanismo de intercomunicación de procesos IPC (Interprocess Communication).

Cuando ejecutas una aplicación, está accede al modo usuario, donde Windows crea un proceso específico para la aplicación. Cada aplicación tiene su dirección virtual privada, ninguna puede alterar los datos que pertenecen a otra y tampoco acceder al espacio virtual del propio sistema operativo. Es por lo tanto el modo que menos privilegios otorga, incluso el acceso al Hardware está limitado, y para pedir los servicios del sistema las aplicaciones tienen que recurrir a la interfaz de programación de aplicaciones API (Application Programming Interface) de Windows.

El modo núcleo en cambio es ese en el que el código que se ejecuta en él tiene acceso directo a todo el Hardware y toda la memoria del equipo. Aquí todo el código comparte un mismo espacio virtual, y puede incluso acceder a los espacios de dirección de todos los procesos del modo usuario. Esto es peligroso, ya que si un Driver en el modo Kernel modifica lo que no debe, podría afectar al funcionamiento de todo el sistema operativo.

Este modo núcleo está formado por servicios Executive, como el controlador de Caché, el gestor de comunicación, gestor de E/S, las llamadas de procedimientos locales, o los gestores de energía y memoria entre otros. Estos a su vez están formados por varios módulos que realizan tareas específicas, controladores de núcleo, un núcleo y una capa de abstracción del Hardware HAL (Hardware Abstraction Layer).

Diferencias entre los Kernel de Linux y Windows La principal diferencia entre el Kernel de los sistemas operativos Windows y el de Linux está en su filosofía. El desarrollado por el equipo de Linus Torvalds es de

código abierto y cualquiera puede usarlo y modificarlo, algo que le sirve para estar presente en múltiples sistemas operativos o distribuciones GNU/Linux. El Kernel de Microsoft[34] en cambio es bastante más cerrado, y está hecho por y para el sistema operativo Windows.

En esencia, en Linux adoptaron los principios de modularidad de Unix y decidieron abrir el código y las discusiones técnicas. Gracias a ello, Linux ha creado una comunidad meritocrática de desarrolladores, una en la que todos pueden colaborar y en la que cada cambio que se sugiere se debate con dureza para desechar las peores ideas y quedarse con las mejores. También se halaga a quienes consiguen mejorar las funcionalidades más veteranas.

Mientras, en Windows no funciona así, los responsables del Kernel no ven con buenos ojos que se hagan propuestas que se desvíen del plan de trabajo, y asegura que hay pocos incentivos para mejorar las funcionalidades existentes que no sean prioritarias.

Esto hace, a ojos de ese antiguo desarrollador, que al dársele mayor importancia a cumplir planes que a aceptar cambios que mejoren la calidad del producto, o al no tener tantos programadores sin experiencia, el Kernel de Windows NT siempre esté un paso por detrás en estabilidad y funcionalidades.

A nivel técnico existen similitudes entre ambos. Los dos núcleos controlan el Software del sistema de bajo nivel y las interacciones con el Hardware del ordenador a través de la capa de abstracción de Hardware (HAL). El HAL es un elemento del sistema que funciona como interfaz entre Software y Hardware, y como las API, permite que las aplicaciones sean independientes del Hardware.

Los dos están escritos principalmente en C, y son capaces de manejar

[34]Para conocer la información del Kernel de Windows usando la línea de comandos podemos utilizar el siguiente comando en un cmd shell:

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

Y en powershell:

```
Get-CimInstance Win32_OperatingSystem | Select-Object Caption, CS-
DVersion, ServicePackMajorVersion, BuildNumber | FL
```

o

```
[System.Environment]::OSVersion.Version
```

el almacenamiento en Caché, los controladores de dispositivos, la memoria virtual, los sistemas de archivos, los protocolos de red y las llamadas de sistema. En esencia sus funcionalidades son las mismas, aunque la manera de llevarlas a cabo es diferente.

Así como el Kernel de Windows tiene dos modos, y por lo tanto se le considera híbrido, la gran diferencia es que el de Linux sólo tiene una capa, o sea que es un núcleo monolítico. Eso sí, pese a ser más sencillo en este aspecto, para funcionar correctamente tiene su núcleo dividido en tres subcapas diferentes.

Ambos gestionan los problemas de memoria de forma parecida. Tienen sistemas de "Swapping" para mover un proceso o parte de él temporalmente de la memoria principal a una secundaria de almacenamiento en el caso de que en la principal haya poco espacio. Windows lo hace en los ficheros Pagefile.sys y Swapfile.sys, mientras que Linux lo suele hacer en una partición, aunque también lo puede hacer en uno o varios ficheros o deshabilitarlo.

Por lo tanto, podemos decir que la principal diferencia entre ambos es la manera en que se desarrolla cada uno. Además, el Kernel de Linux es mucho más sencillo, lo cual es bueno para los desarrolladores. Mientras, el de Windows intenta poner una capa de protección en su modo usuario para que los usuarios con menos conocimientos tengan menos posibilidades de dañar el sistema, y su estructura lo hace más estable frente, por ejemplo a fallos del Driver gráfico.

Pero todo esto ya está cambiando, en las últimas versiones de Windows 10 y 11, Microsoft está integrando el Kernel de Linux a su propio Kernel y esto ha permitido usar Linux dentro de Windows de forma nativa gracias al llamado Windows Subsystem for Linux (WSL, WSL2 WSLg), lo cual ha permitido mejorar la estabilidad y desempeño de Windows.

Kernel de Android Durante la última conferencia de Linux Plumbers 2021, Google dio a conocer sobre el éxito de la iniciativa de mover la plataforma Android para usar un Kernel normal de Linux en lugar de usar su propia versión del Kernel, que incluye cambios específicos para la plataforma Android.

Google menciona que dicho cambio de desarrollo es debido a la decisión de pasar después del año 2023 al modelo «Upstream First», que implica el desarrollo de todas las funciones nuevas del Kernel requeridas en la plataforma Android directamente en el Kernel principal de Linux y no en sus ramas separadas (la funcionalidad será primero se promocionará al Kernel principal

y luego se usará en Android, y no al revés).

Para 2023 y 2024, también se planea transferir al núcleo principal de todos los parches adicionales que quedan en la rama del Kernel común de Android.

En cuanto a un futuro próximo, para la plataforma Android 12 prevista para principios de octubre, se ofrecerán compilaciones del Kernel «Generic Kernel Image» (GKI), lo más parecido posible al Kernel 5.10 habitual.

Para estas compilaciones se proporcionará un lanzamiento regular de actualizaciones, que se colocarán en el repositorio ci.android.com. En el Kernel de GKI, las adiciones específicas de Android, así como los controladores relacionados con el Hardware de los fabricantes de equipos originales, se mueven a módulos de Kernel separados.

Esta nueva interfaz, conocida como Kernel Module Kjos, garantizará que la principal diferencia entre la imagen genérica del Kernel de Android (GKI) y la línea principal de Linux, sean solo los ganchos para todos los módulos específicos del proveedor.

Estos módulos no están vinculados a la versión principal del Kernel y se pueden desarrollar por separado, lo que simplifica enormemente el mantenimiento y la transferencia de dispositivos a nuevas ramas del Kernel. Las interfaces necesarias para los fabricantes de dispositivos se implementan en forma de ganchos que le permiten cambiar el comportamiento del Kernel sin realizar cambios en el código.

En total, el Kernel Android 12-5.10 ofrece 194 ganchos comunes, similares a los puntos de seguimiento, y 107 ganchos especializados que le permiten ejecutar controladores en un contexto no atómico. En el Kernel de GKI, los fabricantes de Hardware tienen prohibido aplicar parches específicos al Kernel principal, y los proveedores deben suministrar los componentes para el Hardware de soporte sólo en forma de módulos de Kernel adicionales, en los que se debe garantizar la compatibilidad con el Kernel principal.

Debemos recordar que la plataforma Android desarrolla su propia rama del Kernel: el «Android Common Kernel», sobre la base del cual se forman las compilaciones específicas separadas para cada dispositivo.

Con lo cual, a partir de cada rama de Android, se proporciona a los fabricantes múltiples diseños de Kernel para sus dispositivos. Por ejemplo, Android 11 ofreció una opción de tres núcleos base a la vez: 4.14, 4.19 y 5.4, y para Android 12, se ofrecerán los núcleos base 4.19, 5.4 y 5.10. La variante 5.10 está diseñada como una imagen de Kernel genérica, en la que las capacidades necesarias para los OEM se transfieren al flujo ascendente, se mueven a módulos o se transfieren al Kernel común de Android.

Antes de la llegada de GKI, el Kernel de Android pasó por varias etapas de preparación:

- La primera de ellas era sobre la base de los principales Kernels LTS (3.18, 4.4, 4.9, 4.14, 4.19, 5.4) y de los cuales se creó una bifurcación del «Android Common Kernel», al que se transferían parches específicos para Android (anteriormente, se alcanzaba el tamaño de los cambios varios millones de líneas).
- Después de ello sobre «Android Common Kernel», los fabricantes de Chips como Qualcomm, Samsung y MediaTek forman el SoC Kernel, que incluye complementos para admitir Hardware.
- Finalmente en el «Kernel de SoC», los fabricantes de dispositivos crean el «Kernel de dispositivo», incluidos los cambios relacionados con la compatibilidad con equipos adicionales, pantallas, cámaras, sistemas de sonido, etc.

Este enfoque complicó significativamente la entrega de actualizaciones con la eliminación de vulnerabilidades y la transición a nuevas ramas del Kernel. Si bien Google publica regularmente actualizaciones para su núcleo común de Android, los proveedores a menudo tardan en enviar estas actualizaciones o usan un solo Kernel durante todo el ciclo de vida del dispositivo, generando una alta fragmentación en el ecosistema Android, una obsolescencia anticipada y en el peor de los casos brechas de seguridad.

Otros Kernels GNU/Linux Actualmente existen una gran cantidad de distribuciones de GNU/Linux que vienen muy optimizadas intentando conseguir la mejor desenvoltura de su arquitectura y configuraciones de serie. En el caso de la configuración por omisión de Debian GNU/Linux y Ubuntu, están pensadas para que sean lo más robusta posible y que se use en todas las circunstancias imaginables, por ello están optimizadas de forma muy conservadora para tener un equilibrio entre eficiencia y consumo de energía. Pero es posible agregar uno o más Kernels GNU/Linux generados por terceros que contenga las optimizaciones necesarias para hacer más eficiente y competitivo en cuestiones de gestión y ahorro de recursos del sistema.

Hay varias opciones del Kernel GNU/Linux optimizado (Liquorix viene optimizado para multimedia y Juegos, por otro lado XanMod tiene uno para propósito general, otro aplicaciones críticas en tiempo real y otro más para

cálculos intensivos) de las últimas versiones estable del Kernel. Estos se pueden instalar[35] mediante el uso de los comandos *dpkg* o *apt* (después de agregarlo a nuestro repositorio */etc/apt/sources.list.d/*), de esta forma siempre podremos tener la última versión del Kernel junto con la actualización básica de nuestro sistema GNU/Linux.

Además, sí instalamos cualquiera de los distintos Kernels, siempre podemos seleccionar alguno de los instalados al momento de arrancar nuestro equipo para usarlo de acuerdo a las actividades requeridas en ese momento. Y en caso necesario, es fácil su desinstalación y continuar usando el Kernel que teníamos por defecto.

Por otro lado, existe una versión completamente libre del Kernel de GNU/Linux (Linux-Libre) el cual es un Kernel despojado de elementos de Firmware y controladores que contienen componentes no libres o fragmentos de código cuyo alcance está limitado por el fabricante.

Linux-libre es el núcleo recomendado por la Free Software Foundation y una pieza principal de las distribuciones GNU totalmente libres de fragmentos privativos o Firmwares incluidos en Linux sirven para inicializar los dispositivos o aplicarles parches que solventan fallas del Hardware que no pudieron ser corregidas antes de ser puestos a disposición de los usuarios.

Además, Linux-libre deshabilita las funciones del Kernel para cargar componentes no libres que no forman parte del suministro del Kernel y elimina la mención del uso de componentes no libres de la documentación. El Kernel de Linux-libre se utiliza en distribuciones como Dragora Linux, Trisquel, Dyne, Bolic, gNewSense, Parabola, Musix y Kongoni.

Estabilidad del Kernel La estabilidad de un núcleo no es tan difícil. El Kernel de Unix de Mac o el Kernel de Linux están diseñados de manera diferente pero resuelven el mismo problema. El sistema operativo Windows es igualmente robusto. Eso es evidente.

Pero la estabilidad real del día a día depende de otros factores. Particularmente en los controladores que conectan el sistema operativo al Hardware. Aquí es donde surgen las diferencias.

Apple tiene el momento más fácil, porque solo admiten un pequeño conjunto de Hardware seleccionado. Eso facilita su trabajo, el objetivo es pequeño. Apple ocasionalmente estropea esto, pero en su mayor parte, OS X

[35] Para ver las opciones de optimización del Kernel y como instalarlo ver la página Web de cada proyecto: Liquorix, XanMod, Linux-Libre.

ofrece una notable estabilidad diaria para las aplicaciones de escritorio.

Windows tiene un trabajo mucho más difícil. El sistema operativo admite una gama simplemente gigantesca de Hardware, y los fabricantes de Hardware hacen todo lo posible para proporcionar controladores de alta calidad. Este es el valor real de Windows, como paquete de controladores, es prácticamente imbatible.

Linux también intenta admitir una gran variedad de Hardware. Pero muchos fabricantes de Hardware son absolutamente indiferentes a la compatibilidad con Linux. Por lo tanto, el soporte de Hardware en Linux es mucho más impredecible. Si está ejecutando un servidor en Linux y el sistema solo se comunica con un disco duro y un adaptador de red, es probable que tenga una estabilidad impecable que supere a la industria.

Pero, si instala Linux en una computadora portátil y espera que funcione con la función de reposo / activación, la GPU, la tarjeta de sonido y un montón de extravagantes periféricos, entonces podría alejarse del rango de la estabilidad. Hay algunos controladores de código abierto, pero estos son significativamente peores que las versiones de los fabricantes. Por ejemplo, una GPU puede ser 4 o 5 veces más lenta.

Como usuario de escritorio de Linux, es probable que también instale aplicaciones que hacen cosas interesantes, de diversos proveedores, que pueden no estar del todo de acuerdo con las mejores prácticas.

Las Vulnerabilidades y Exposiciones Comunes El mundo está cada vez más interconectado y, como resultado de esto, la exposición a las vulnerabilidades de seguridad también ha aumentado dramáticamente. Las complejidades de mantener las plataformas de cómputo actuales hacen que sea muy difícil para los desarrolladores cubrir cada punto de entrada potencial. En 2019 hubo un promedio de más de 45 vulnerabilidades y exposiciones comunes registradas por día y estas siguen en aumento año con año.

Las vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures, CVE https://cve.mitre.org) que tienen los distintos sistemas operativos, es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, que versiones del Software están afectadas, posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o Blogs donde se ha hecho pública la vulnerabilidad o se demues-

tra su explotación. Además suele también mostrarse un enlace directo a la información de la base de datos de vulnerabilidades (https://nvd.nist.gov, https://openssf.org y https://docs.aws.amazon.com/security), en la que pueden conseguirse más detalles de la vulnerabilidad y su valoración.

El CVE-ID ofrece una nomenclatura estándar para identificación de la vulnerabilidad de forma inequívoca que es usada en la mayoría de repositorios de vulnerabilidades. Es definido y es mantenido por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

Mitos en torno a Linux/Unix Hay varios mitos en torno a Linux/Unix y al Software libre, a saber:

- Linux/Unix se puede usar para revivir un equipo de cómputo viejo. La realidad es que si bien, hay múltiples distribuciones de Linux/Unix que corren en una gran cantidad de procesadores antiguos y actuales, los Drivers necesarios para reconocer periféricos como tarjetas gráficas, de red alámbrica e inalámbrica, entre muchos otros, no tienen soporte en Linux/Unix, lo cual hará imposible su uso en Linux/Unix. Esto es cierto en cualquier computadora no importa de cuál generación es el equipo de cómputo. La verdad de todo esto, es que los fabricantes están enfocados en producir Hardware y Drivers que corran en los sistemas operativos con mayor cuota de mercado y por el momento Linux/Unix en equipos personales no son de ellos.

- La compatibilidad del Hardware depende en gran medida de la versión de Kernel de GNU/Linux instalado, es de esperarse que en versiones anteriores del Kernel cierto Hardware no se pueda detectar, pero lo contrario también pasa, hay Drivers que solo corren correctamente en versiones anteriores del Kernel y no en las últimas versiones, lo que ocasiona que muchos usuarios se desesperen al tratar de usar sus equipos con GNU/Linux. Y en caso de logar que funcione el Hardware, se fuerza a los usuarios a usar una determinada versión del Kernel (y todas las aplicaciones de la distribución) no actualizable, por la imposibilidad de hacer funcionar el Hardware del equipo en una más moderna con la consiguiente obsolescencia del Software instalado en el equipo.

- Si tengo un Software ahora y quiero ejecutarlo dentro de cinco o diez años en el futuro ¿Por qué no debería ser capaz de hacerlo? Parte de la belleza del Open Source es que el código fuente está disponible, por lo que es más fácil mantener operativo el Software, de modo que no deje de funcionar cuando alguien deja de mantenerlo. Excepto que mantener el Software en Linux/Unix se está convirtiendo en un desafío tan grande que daría igual que fuese privativo. Porque sería complicado hacerlo funcionar en un tiempo razonable, incluso siendo desarrollador, podría costar mucho trabajo y es posible dejar algo sin funcionar en el camino.

- La retrocompatibilidad[36] es un enorme dolor de cabeza, tomar Software hecho para Linux/Unix de hace 10 o 5 años y ejecutarlo en una distribución moderna. Cualquier cosa de mínima complejidad o que use una GUI, simplemente no funciona. Mientras la retrocompatibilidad en Windows es simplemente increíble. En Linux/Unix somos dependientes de los repositorios en línea, y cuando una aplicación depende de ciertas librerías que empiezan a desaparecer de esos repositorios, nos encontramos en una pesadilla. Y mientras más viejo el Software, peor.

2.1 Windows

Microsoft Windows (véase [1]), conocido generalmente como Windows o MS Windows es el nombre de una familia de Software propietario (véase apéndice 11.1) de distribuciones de Software para PC, Smartphone -que perdió cuota de mercado con Android hasta desaparecer-, servidores y sistemas empotrados, desarrollados y vendidos por Microsoft y disponibles para múltiples arquitecturas, tales como x86, x86-64 y ARM.

Desde un punto de vista técnico, no son sistemas operativos, sino que contienen uno (tradicionalmente MS-DOS, o el más actual, cuyo núcleo es Windows NT) junto con una amplia variedad de Software; no obstante, es usual (aunque no necesariamente correcto) denominar al conjunto como sistema operativo en lugar de distribución.

[36] Siempre estamos en posibilidad de usar una Máquina Virtual que nos permite usar un programa desarrollado hace años o décadas en su entorno original, corriendo en un equipo moderno con un sistema operativo de última generación con todas las actualizaciones de seguridad pertinentes.

La versión más reciente de Windows es Windows 11 para equipos personales (que se ofrece como actualización gratuita para los equipos con licencia válida de Windows 10 que cumplan con los requisitos mínimos de Hardware exigidos), Windows Server 2022 para servidores.

Windows 11 tiene al menos siete ediciones con diferente conjunto de características y Hardware previsto, algunas de ellas son: Home, Pro, Pro Education, Pro for Workstations, Enterprise, Education, Mixed Reality. Además habrá un modo SE para hacer frente al Chrome OS de los Chromebooks de Google.

Windows 11 también se puede descargar como una imagen ISO para instalaciones nuevas, ejecución en máquinas virtuales, además de ser la versión de referencia que los fabricantes OEM que usarán para preinstalaciones en equipos nuevos.

Por su parte, Windows 10 tiene al menos doce ediciones con diferente conjunto de características y Hardware previsto, algunas de ellas son: Home, Pro, Enterprise, Enterprise LTBS/LTSC, Education, Mobile, S, Pro for Workstation, Team, Pro Education, loT (Embedded), N y KN. Se espera que cuente con soporte y actualizaciones hasta el 2025.

Todas las ediciones mencionadas tienen la capacidad de utilizar los paquetes de idiomas, lo que permite múltiples idiomas de interfaz de usuario. A pesar de la múltiple cantidad de ediciones, solamente Windows Home y Pro están orientadas para el común de los usuarios y vienen instaladas en equipos nuevos. Las demás ediciones se adquieren mediante otros tipos de compra.

Por su parte, Windows 10 llegó de forma oficial y gratuita a usuarios con licencia genuina de Windows 7, Windows 8.1 y Windows 8 así como a Insiders, siendo la primera versión que buscaba la unificación de dispositivos (escritorio, portátiles, teléfonos inteligentes, tabletas y videoconsolas) bajo una experiencia común, con lo que se esperaba eliminar algunos problemas que se presentaron con Windows 8.1.

Además está Windows PE que es un pequeño sistema operativo usado para instalar, desplegar y reparar Windows 10 en todas sus versiones de escritorio, servidor y para otras ediciones de Windows. En concreto, podemos preparar el disco antes de la instalación, instalar Windows con apps desde un disco local o una red, instalar imágenes de Windows, hacer modificaciones en Windows sin iniciar sesión, recuperar datos perdidos y un largo etcétera.

Seguridad Una de las principales críticas que reciben los sistemas operativos Windows es la debilidad del sistema en lo que a seguridad se refiere y el alto índice de vulnerabilidades críticas. El propio Bill Gates, fundador de Microsoft, ha asegurado en repetidas ocasiones que la seguridad es objetivo primordial para su empresa.

Partiendo de que no existe un sistema completamente libre de errores, las críticas se centran en la lentitud con la que la empresa reacciona ante un problema de seguridad que pueden llegar a meses o incluso años de diferencia desde que se avisa de la vulnerabilidad hasta que se publica la actualización que corrija dicha vulnerabilidad (parche). En algunos casos la falta de respuesta por parte de Microsoft ha provocado que se desarrollen parches que arreglan problemas de seguridad hechos por terceros.

Uno de los pilares en que se basa la seguridad de los productos Windows es la seguridad por ocultación, en general, un aspecto característico del Software propietario que sin embargo parece ser uno de los responsables de la debilidad de este sistema operativo debido a que, la propia seguridad por ocultación, constituye una infracción del uno de los principios de Kerckhoffs, el cual afirma que la seguridad de un sistema reside en su diseño y no en una supuesta ignorancia del diseño por parte del atacante.

Windows 11 Microsoft presentó el 24 de junio del 2021 la siguiente generación de su sistema operativo y que se puede descargar como actualización a partir del 5 de octubre del 2021. Windows 11 con un nuevo diseño que potencia las formas redondeadas y las transparencias, y enfocado a la productividad. Este diseño, que incluye un modo oscuro y uno claro, está pensado para transmitir sensación de calma y sobre todo para que el usuario tenga la información siempre a mano. Esto se aprecia en nuevas funciones, como los Widgets, que pueden personalizar tarjetas de información sobre el tiempo, el tráfico, o información local.

La compañía también ha rediseñado el menú de inicio y la barra de tareas con el acceso a aplicaciones como Teams, que ahora está integrado en Windows. Con Snap Layouts, Windows 11 permite personalizar la apariencia y la disposición de las ventanas. El usuario también podrá personalizar escritorios según el uso, ya sea para el trabajo, para el estudio o el ocio, con configuraciones separadas.

La nueva experiencia con las aplicaciones y son el 'Docking' –cuando el portátil se conecta a un monitor– hacen posible retomar el trabajo, incluso

con varias aplicaciones abiertas, en el mismo lugar donde el usuario lo dejó antes de apartarse del ordenador. Windows 11 también está diseñado para que siempre se sienta igual tanto si se usa en una tableta y su pantalla táctil como si se usa en un ordenador con teclado. Además, mejora la experiencia con el lápiz óptico y teclado táctil en pantalla.

Otro elemento que presenta novedades es Microsoft Store, que ha sido rediseñada para facilitar la búsqueda de aplicaciones, e incorpora también las aplicaciones de Android, que pueden colocarse en la barra de tareas. Con Windows 11 se tendrá una nueva tienda de aplicaciones, una que abrirá sus puertas a todo tipo de aplicaciones y juegos. Esto quiere decir que a partir de ahora la nueva generación de Windows contará con PWA (aplicaciones Web progresivas), UWP (aplicaciones universales) y los programas clásicos Win32 en un mismo lugar.

En cuanto al tema de actualizaciones, Microsoft abandona definitivamente el programa de entrega de actualizaciones semestrales de Windows 10 que definitivamente no pudo concretar con la estabilidad requerida. Windows 11 solo recibirá una actualización anual de características, funciones y soporte de nuevas tecnologías, lo que debería otorgarle tiempo suficiente para desarrollo y pruebas, entregando versiones más pulidas. Las actualizaciones acumulativas de seguridad y corrección de errores si mantendrán el actual ciclo de entrega mensual.

En octubre del 2022 se publicó[37] que Windows 10 se mantiene con una cuota de mercado de 71.29%, mientras que Windows 11 tiene una cuota de 15.44%, esta diferencia deduce por los altos requisitos mínimos de Hardware exigidos -4 GB RAM, TPM 2.0 y 60 GB de Disco-. Por otra parte, las cuotas de mercado de las versiones sin soporte de Windows son: Windows 8.1 de 2.45%, Windows 8 de 0.69%, Windows 7 de 9.61% y Windows XP de 0.39%.

Windows 365 Microsoft presentó en julio del 2021 la nueva versión de Windows en la nube que llevará el nombre de Windows 365. Este nuevo servicio de suscripción, está especialmente dirigido a empresas, que permitirá acceder a nuestra sesión de usuario desde cualquier equipo (el PC, el Mac, la tableta o teléfono Android, etc.), pues el Software y el sistema de

[37] Cuotas de mercado de diferentes sistemas operativos:

https://gs.statcounter.com/os-market-share/desktop/worldwide
https://netmarketshare.com

archivos están alojados en una máquina virtual remota, por lo que la configuración, documentos y herramientas disponibles serán idénticos desde donde accedamos.

Así, desde cualquier navegador (o bien usando la aplicación de Escritorio Remoto de Windows) podremos acceder a un Windows 11/10 disfrutando de una experiencia de arranque casi instantáneo, pero esa no será la única ventaja de esta plataforma. Aún más importante será la posibilidad de contar con varios 'ordenadores' en una misma cuenta, cada uno con distinta potencia (RAM, núcleos de procesador...) y capacidad de almacenamiento contratada, según el trabajo que necesitemos llevar a cabo en cada momento.

Microsoft ya ha confirmado que ofrecerá 12 configuraciones de Hardware distintas para sus equipos virtualizados (iniciando en $130 pesos mexicanos por mes). Así, las empresas podrán 'crear PCs' en cuestión de minutos y asignar cada uno a un empleado, eliminando los inconvenientes que conlleva el hecho de manejar Hardware físico.

Windows 11 SE Microsoft anunció en noviembre del 2021 el lanzamiento de una nueva versión de Windows 11 que hará compañía a las versiones 'Pro' y 'Home': su nombre es Windows 11 SE, llevábamos oyendo rumores al respecto desde junio y desembarca ahora para hacer frente al Chrome OS de los Chromebooks de Google, por lo que se destinará únicamente en portátiles escolares de bajo costo.

El sistema estará optimizado para su uso con MS Edge, MS Office y el resto de servicios de la nube de Microsoft, estará abierto a muchas más aplicaciones de terceros. En palabras de Paige Johnson, directora de marketing educativo de Microsoft, "Windows 11 SE también es compatible con aplicaciones de terceros, incluidas Zoom y Chrome, porque queremos dar a las escuelas la opción de usar lo que funcione mejor para ellas".

Winget Windows Package Manager (*winget*) es el gestor de paquetes de Windows 11 y 10 que permite usar comandos desde la terminal para instalar aplicaciones de forma rápida y sencilla (al más puro estilo de Linux). El único requisito para instalar *winget* es contar con Windows 10 1890 o versión posterior, es posible usar para actualizar una o todas las aplicaciones del sistema usando:

C: winget upgrade –all

también es posible usar *WInstall* interfaz gráfica no oficial de *winget* para elegir programas en un click desde una Web y luego instalarlos en Windows con *winget* con la misma rapidez y automatización.

Microsoft Open Source En Agosto del 2020 presentó la empresa de Redmond el nuevo sitio Microsoft Open Source en que el público puede navegar a través de todo el ecosistema de código abierto que ha estado construyendo en los últimos años. La Web no solo muestra los proyectos Open Source de Microsoft sino que cuenta con secciones para colaborar con la comunidad, descargar herramientas, explorar su código, y hasta encontrar oportunidades de trabajo.

Las dos partes más importantes de este nuevo sitio son las secciones "Get involved" y "Explore proyects". En la primera se puede revisar toda la actividad reciente en los proyectos Open Source de Microsoft alojados en GitHub, y además se cuenta con una larga lista de recursos para aprender a colaborar con proyectos de código abierto, y no necesariamente solo los que mantiene Microsoft.

La segunda sección es la lista de proyectos, y ahí nos encontramos los principales proyectos Open Source mantenidos por los ingenieros de Microsoft y la comunidad. La lista de proyectos es larga y podemos encontrar los proyectos de los empleados de la empresa patrocinados a través de Microsoft FOSS Fund.

Linux Dentro de Windows Desde el 2018 se inició la integración de GNU/Linux en Windows 10, con la actualización de Windows 10 Fall Creator Update con WSL (Windows Subsystem for Linux), se permitía instalar consolas de diversas distribuciones de GNU/Linux como un programa más. Y en el 2020, con la llegada de Windows 10 Build 2020 con WSL2, el cual cuenta con su propio Kernel de Linux que permite instalar de manera casi nativa diversas distribuciones de GNU/Linux con todo el ambiente gráfico permitiendo tener lo mejor de ambos mundos en un mismo equipo -sin hacer uso de programas de virtualización-, incluso es posible ejecutar varias distribuciones de Linux al mismo tiempo en pantalla.

Para usarlo hay que tener todas las actualizaciones de Windows y activar el Subsistema de Windows para Linux (WSL[38]). Reiniciando el sistema, ya podemos usar distribuciones de Linux desde Microsoft Store.

[38] https://docs.microsoft.com/en-us/windows/wsl/install-win10

En el Windows Insider Preview Build 20150 ha incluido soporte para GPU de Intel, AMD y NVIDIA y es compatible con Direct ML (una API de bajo nivel para aprendizaje automático soportado por DirectX 12) permitiendo el uso de las capacidades de computación por GPU de WSL para Linux.

En abril del 2021 se anunció la llegada de WSLg en la que se pueden correr aplicaciones (como gedit, Audacity, etc.) e IDEs con soporte para X11 y Wayland, PulseAudio de Linux con GUI (Graphical User Interface) con soporte para gráficos 3D acelerados por Hardware de forma independiente de la distribución de Linux en la que se instalaron, esta novedad está disponible a partir de la versión Windows Insider Preview Build 21364 y para todos los usuarios en Windows 10 May 2020 Update.

Android Dentro de Windows En el Windows Build 20185 ha incluido soporte para que Windows 10 permite no sólo sincronizar teléfonos Android, sino además mediante "your Phone" permite integrar las aplicaciones, notificaciones, mensajes, fotos, llamadas y otras opciones de teléfonos inteligentes en Android directamente en Windows, ejecutando las aplicaciones sin tener que abrirlas en el teléfono, aunque siguen proviniendo de ahí.

Además en noviembre de 2020, se ha informado que existe la posibilidad de que Microsoft permita la instalación y ejecución de aplicaciones para Android en Windows 11. Con cambios mínimos o directamente sin modificaciones en el código, los desarrolladores podrían enviar a Microsoft Store sus aplicaciones para que sean descargadas e instaladas en PCs, el proyecto tiene el nombre de Latte.

Microsoft Azure Durante los últimos años, Microsoft ha declarado en conferencias magistrales de eventos y en otros lugares que Linux es un sistema operativo de rápido crecimiento que se usa dentro de Microsoft Azure.

Han declarado con orgullo que el 50 % de las máquinas virtuales nuevas que se ejecutaban en Azure ejecutaban Linux. En Octubre del 2022, las estadísticas reportadas señalan:

- Más del 50 % de los núcleos de máquinas virtuales ejecutan Linux en Azure
- Las imágenes basadas en Linux comprenden el 60 % de las imágenes de Azure Marketplace

- Los 100 principales clientes de Microsoft implementan cargas de trabajo de Linux en Azure
- Azure Tuned Kernels proporciona un rendimiento de red un 25 % más rápido
- Microsoft es compatible con todas las principales distribuciones de Linux, como: Red Hat, SUSE, Ubuntu, Oracle Linux, Debian, CentOS, CoreOS y OpenSUSE (Relacionado: Azure también es compatible con FreeBSD)
- Azure ofrece dos servicios de orquestación de Kubernetes administrados con soporte nativo: Azure Kubernetes Service y Azure Red Hat OpenShift

2.2 UNIX y BSD

Unix (véase [3]) es un sistema operativo portable, multitarea y multiusuario; desarrollado en 1969 por un grupo de empleados de los laboratorios Bell de AT&T. El sistema, junto con todos los derechos fueron vendidos por AT&T a Novell Inc. Esta vendió posteriormente el Software a Santa Cruz Operation en 1995, y está, a su vez, lo revendió a Caldera Software en 2001, empresa que después se convirtió en el grupo SCO. Sin embargo, Novell siempre argumentó que solo vendió los derechos de uso del Software, pero que retuvo el Copyright sobre "UNIX". En 2010, y tras una larga batalla legal, esta ha pasado nuevamente a ser propiedad de Novell.

Solo los sistemas totalmente compatibles y que se encuentran certificados por la especificación Single UNIX Specification pueden ser denominados "UNIX" (otros reciben la denominación «similar a un sistema Unix»). En ocasiones, suele usarse el término "Unix tradicional" para referirse a Unix o a un sistema operativo que cuenta con las características de UNIX Versión 7 o UNIX System V o UNIX versión 6.

Berkeley Software Distribution o BSD (en español, «distribución de Software Berkeley») (véase [4]) fue un sistema operativo derivado de Unix que nace a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley. En los primeros años del sistema Unix sus creadores, los Laboratorios Bell de la compañía AT&T, autorizaron a la Universidad de Berkeley en California y a otras universidades, a utilizar el código fuente y

adaptarlo a sus necesidades. Durante los años 1970 y 1980 Berkeley utilizó el sistema para sus investigaciones en materia de sistemas operativos.

Cuando AT&T retiró el permiso de uso a la universidad por motivos comerciales, la universidad promovió la creación de una versión inspirada en el sistema Unix utilizando los aportes que ellos habían realizado, permitiendo luego su distribución con fines académicos y al cabo de algún tiempo reduciendo al mínimo las restricciones referente a su copia, distribución o modificación (véase apéndice 11.4).

Algunos sistemas operativos descendientes del sistema desarrollado por Berkeley son SunOS, FreeBSD, NetBSD, OpenBSD, DragonFlyBSD y Mac Big Sur. BSD también ha hecho grandes contribuciones en el campo de los sistemas operativos en general. Además, la licencia permisiva de BSD ha permitido que otros sistemas operativos, tanto libres como propietarios incorporaron código BSD. Por ejemplo, Microsoft Windows ha utilizado código derivado de BSD en su implementación de TCP/IP, y utiliza versiones recompiladas de la línea de comandos BSD para las herramientas de redes. También Darwin, el sistema en el cual está construido Mac Big Sur, el sistema operativo de Apple, está derivado en parte de FreeBSD 5. Otros sistemas basados en Unix comerciales como Solaris también utilizan código BSD.

Algunos proyectos activos descendientes del sistema BSD son:

FreeBSD (https://www.freebsd.org/es/)
Es un sistema operativo para computadoras basadas en las CPU de arquitectura Intel. También funciona con procesadores compatibles como AMD. Está basado en la versión 4.4 BSD-Lite del CSRG (Computer Systems Research Group) y fue escrito en C y C++. Tiene Licencia BSD. Este proyecto ha realizado una gran inversión de tiempo en ajustar el sistema para ofrecer las mejores condiciones de rendimiento con carga real y facilidad de uso al usuario final.

NetBSD (https://www.netbsd.org)
Está basado en un conjunto de aplicaciones Open Source, incluyendo 4.4 BSD-Lite de la Universidad de California en Berkeley, Net/2 (Berkeley Networking Release 2), el sistema gráfico X del MIT y aplicaciones del proyecto GNU. Tiene Licencia BSD. NetBSD ha invertido sus energías en proveer de un sistema operativo estable, multiplataforma, seguro y orientado a la inves-

tigación. Está portado a 56 arquitecturas de Hardware y suele ser el primero en implementar tecnologías nuevas, como IPv6.

OpenBSD (https://www.openbsd.org)
Está basado en 4.4 BSD y es un descendiente de NetBSD. El proyecto tiene el foco puesto de forma particular en la seguridad y criptografía. Los esfuerzos se centran en la portabilidad, cumplimiento de normas, corrección, seguridad y criptografía integrada. Tiene Licencia BSD. La filosofía del proyecto puede ser descrita en tres palabras: "Free, Functional and Secure" (Libre, Funcional y Seguro).

DragonFlyBSD (https://www.dragonflybsd.org)
Tiene como meta ofrecer un alto rendimiento y escalabilidad bajo cualquier entorno, desde computadoras de un solo usuario hasta enormes sistemas de clústeres. DragonFlyBSD tiene varios objetivos técnicos a largo plazo, pero el desarrollo se centra en ofrecer una infraestructura habilitada para SMP que sea fácil de entender, mantener y desarrollar.

2.3 Apple y sus macOS e iOS

Apple a la empresa multinacional estadounidense Apple Inc., dedicada al diseño, la confección y la comercialización de productos electrónicos y de Software, así como de los servicios en línea (a través de Internet) que los atañen. Es considerada como una de las sociedades más apreciables del mundo. Su función principal es la producción de aparatos digitales populares, las marcas más populares de esta compañía son: Mac, iPods, iPads e iPhones. Y cuya gama de productos ha ganado un nicho particular en el área de los Gadgets tecnológicos mediante su estética común, intensa mercadotecnia y pretendida alternatividad respecto a otras empresas hegemónicas como Microsoft.

En la actualidad los principales productos de Apple gozan de una amplia popularidad a nivel mundial, particularmente en lo vinculado con reproductores de música, computadores personales, tabletas, teléfonos, relojes inteligentes, Wearables y toda una red de Software que va desde sistemas operativos, programas de gestión de multimedios (como iTunes) o suites de edición profesional. Se trata de una empresa líder en innovación tecnológica y computarizada.

El sistema de Apple siempre se ha caracterizado por contar con detalles no solo sofisticados, sino también fuera de lo común, tratando de marcar la historia de la tecnología bajo Software con distintas mejoras, asistentes virtuales y muchos elementos que dejan gran satisfacción y que debes conocer.

Realizando un seguimiento de los últimos productos lanzados y presentados por los chicos de la manzanita nos damos cuenta de que sin duda son los mejores creando expectación. En Apple saben que para vender hay que mostrar cosas nuevas e innovar, ya que vivimos en un mundo en el que la tecnología evoluciona constantemente y si no lo haces, te quedas atrás. Pero..., ¿siempre son cosas nuevas las que nos muestran?.

Una de las cosas en las que destaca Apple por encima de sus competidores es en el campo de la investigación y la innovación. Las inversiones que realiza la empresa más valiosa del mundo en investigación son enormes, y no en vano. Porque si algo sabe hacer bien Apple es ir por delante de la competencia. En esto todos estamos de acuerdo, los de Cupertino saben mejor que nadie que innovar significa no tener competencia en el mercado. Sin duda, esto saben aprovecharlo y a veces, de tal manera que ni nos damos cuenta.

Pero en Apple tienen una fea costumbre que analizando un poco las últimas Keynotes nos damos cuenta. Los de Cupertino suelen vender como algo innovador y único cosas que ya hacía antes pero pasaba por alto. ¿Qué significa esto?, que en Apple saben como vender las características de sus productos para que nos parezcan espectaculares.

Las computadoras de Apple tienen un sistema operativo único y otras características que sólo están disponibles en las Macs. El diseño del Hardware de Apple unifica la marca, con productos como el iMac "todo en uno", el iMac original con sus colores brillantes y la gama de computadoras portátiles. Además, las nuevas características del sistema operativo que integran el uso de una computadora Mac, iPad, el teléfono o el iPod con iTunes de Apple y la tienda de aplicaciones, proporcionan a los clientes una experiencia de Apple aerodinámica.

Características de Mac

- Carpetas inteligentes en Finder
- Grabe la actividad de la pantalla macOS en QuickTime
- Activa las esquinas calientes de tu pantalla

- Reproduce música y películas
- Ejecutar Windows con Boot Camp
- Automatiza las tareas repetitivas
- Crea escritorios virtuales
- Ping archivos de forma inalámbrica con AirDrop
- Firmar documentos en Vista previa
- Autocompletar palabras a medida que escribe

Características de iOS

- Notificaciones innovadoras
- Widgets de máxima utilidad
- Puedes borrar las aplicaciones de fábrica
- Siri abre apps de terceros
- Varios idiomas para el teclado
- Reconocimiento facial en sus fotos
- Te permite controlar tu hogar
- 3D touch con muchos usos
- Dispone de mensajería interna: iMessage

Mac OS y macOS Ventura Mac OS (véase [5]) -del inglés Macintosh Operating System, en español Sistema Operativo Macintosh- es el nombre del sistema operativo propietario (véase apéndice 11.1) creado por Apple para su línea de computadoras Macintosh, también aplicado retroactivamente a las versiones anteriores a System 7.6, y que apareció por primera vez en System 7.5.1. Es conocido por haber sido uno de los primeros sistemas dirigidos a un gran público al contar con una interfaz gráfica compuesta por la interacción del Mouse con ventanas, íconos y menús.

Debido a la existencia del sistema operativo en los primeros años de su línea Macintosh resultó a favor de que la máquina fuera más agradable al usuario, diferenciándolo de otros sistemas contemporáneos, como MS-DOS, que eran un desafío técnico. El equipo de desarrollo del Mac OS original incluía a Bill Atkinson, Jef Raskin y Andy Hertzfeld.

Este fue el comienzo del Mac OS clásico, desarrollado íntegramente por Apple, cuya primera versión vio la luz en 1985. Su desarrollo se extendería hasta la versión 9 del sistema, lanzada en 1999. A partir de la versión 10 (Mac OS X), el sistema cambió su arquitectura totalmente y comenzó a basarse en BSD Unix, sin embargo su interfaz gráfica mantiene muchos elementos de las versiones anteriores.

Hay una gran variedad de versiones sobre cómo fue desarrollado el Mac OS original y dónde se originaron las ideas subyacentes. Pese a esto, los documentos históricos prueban la existencia de una relación, en sus inicios, entre el proyecto Macintosh y el proyecto Alto de Xerox PARC. Las contribuciones iniciales del Sketchpad de Ivan Sutherland y el On-Line System de Doug Engelbart también fueron significativas.

Versiones Antes de la introducción de los últimos sistemas basados en el microprocesador PowerPC G3, partes significativas del sistema se almacenaban en la memoria física de sólo lectura de la placa base. El propósito inicial de esto fue evitar el uso de la capacidad de almacenamiento limitada de los disquetes de apoyo al sistema, dado que los primeros equipos Macintosh no tenían disco duro. Sólo el modelo Macintosh Classic de 1991, podía ser iniciado desde la memoria ROM.

Esta arquitectura también permitió una interfaz de sistema operativo totalmente gráfica en el nivel más bajo, sin la necesidad de una consola de sólo texto o el modo de comandos de línea. Los errores en tiempo de arranque, como la búsqueda de unidades de disco que no funcionaban, se comunicaban al usuario de manera gráfica, generalmente con un ícono o con mensajes con el tipo de letra Chicago y un "timbre de la muerte" o una serie de pitidos.

Esto contrastaba con los PCs de la época, que mostraban tales mensajes con un tipo de letra monoespaciada sobre un fondo negro, y que requerían el uso del teclado y no de un ratón, para el acceso. Para proporcionar tales detalles en un nivel bajo, Mac OS dependía del Software de la base del sistema grabado en la ROM de la placa base, lo que más tarde ayudó a garantizar que sólo los equipos de Apple o los clones bajo licencia (con el contenido de la

memoria ROM protegido por derechos de autor de Apple, pudieran ejecutar Mac OS).

Mac OS puede ser dividido en tres familias:

- La familia Mac OS Classic, basada en el código propio de Apple Computer.
- El Sistema Operativo Mac OS X, desarrollado a partir de la familia Mac OS Classic y NeXTSTEP, el cual estaba basado en UNIX.
- MacOS Ventura es el reemplazo de macOS Monterrey (que fue el reemplazo de Mac OS X), disponible a partir de junio del 2022, que usando los procesadores de ARM han mostrado un gran desempeño en comparación con equipos INTEL y AMD de gama alta.

Linux Dentro de IOS Es posible tener un Linux completo en IOS además de poder hacer uso de Secure Shell (SSH) a una computadora con Linux. Para la primera forma, se puede ejecutar un sistema virtualizado utilizando Alpine Linux con iSH, que es de código abierto, pero debe instalarse utilizando la aplicación TestFlight propiedad de Apple.

Alternativamente hay aplicaciones de emulador de terminal de código abierto que proporcionan herramientas de código abierto dentro de un entorno restringido. Esta es la opción más limitada -en realidad no nos permite ejecutar Linux, pero estaremos ejecutando herramientas de Linux- pero brindan algunas funciones de línea de comandos. Por ejemplo:

- Sandboxed Shell, con más de 80 comandos e incluye Python 2 y 3, Lua, C, Clang, etc.
- a-Shell, otorga acceso al sistema de archivos e incluye Lua, Python, Tex, Vim, JavaScript, C yC++, junto con Clang y Clang++; y permite instalar paquetes de Python con pip.
- Blink Shell, permite la conexión con servidores.
- iSH, es un Shell Linux que usa *usermode x86* emulación y traducciones de *syscall*.

2.4 GNU/Linux

GNU[39]/Linux (véase [2]) también conocido como Linux, es un sistema operativo libre (véase apéndice 11.2) tipo Unix; multiplataforma, multiusuario y multitarea. El sistema es la combinación de varios proyectos, entre los cuales destacan GNU (encabezado por Richard Stallman y la Free Software Foundation) y el núcleo Linux (encabezado por Linus Torvalds). Su desarrollo es uno de los ejemplos más prominentes de Software libre: todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera, bajo los términos de la GPL (Licencia Pública General de GNU) y otra serie de licencias libres.

A pesar de que «Linux» se denomina en la jerga cotidiana al sistema operativo, este es en realidad solo el Kernel (núcleo) del sistema. La idea de hacer un sistema completo se remonta a mediados de la década de 1980 con el proyecto GNU, así como una gran cantidad de los componentes que se usan hoy en día -además del núcleo-, que van desde los compiladores de GNU hasta entornos de escritorio. Sin embargo, tras la aparición de Linux en la década de 1990 una parte significativa de los medios generales y especializados han utilizado el término «Linux» para referirse a todo. Esto ha sido motivo de polémicas. Cabe señalar que existen derivados de Linux que no tienen componentes GNU -por ejemplo Android-, así como distribuciones de GNU donde Linux está ausente -por ejemplo Debian GNU/Hurd-.

A GNU/Linux se le encuentra normalmente en forma de compendios conocidos como distribuciones o distros, a las cuales se les ha adicionado selecciones de aplicaciones y programas para descargar e instalar las mismas. El propósito de una distribución es ofrecer GNU/Linux como un producto final que el usuario pueda instalar, cumpliendo con las necesidades de un grupo de usuarios o bien del público en general. Algunas de ellas son: Ubuntu, CentOS, Debian, Linux Mint, Arch Linux, Fedora, Red Hat, Oracle, Zorin, MX Linux, Parrot, Manjaro, Elementary, etc.

Algunas de ellas son especialmente conocidas por su uso en servidores de internet y supercomputadoras -donde GNU/Linux tiene la cuota más importante del mercado. Según el informe de International Data Corporation (IDC), GNU/Linux es utilizado por los más poderosos 500 sistemas de super-

[39] GNU -es un acrónimo recursivo de «GNU no es UNIX»- es un sistema operativo de Software libre, es decir, respeta la libertad de los usuarios. El sistema operativo GNU consiste en paquetes de GNU además de Software libre publicado por terceras partes con distintas licencias que conforman una distribución.

cómputo de alto desempeño del mundo[40]-, en cuanto a teléfonos inteligentes y tabletas tiene una cuota de 86% y con menor participación, el sistema GNU/Linux también se usa en el segmento de las computadoras de escritorio, portátiles, computadoras de bolsillo, sistemas embebidos, videoconsolas y otros dispositivos.

Creación El proyecto GNU, iniciado en 1983 por Richard Stallman, tiene el objetivo de crear un «sistema de Software compatible con Unix compuesto enteramente de Software libre». El trabajo comenzó en el año 1984. Más tarde, en 1985, Stallman fundó la Free Software Foundation para financiar el desarrollo de GNU, y escribió la Licencia Pública General de GNU en 1989. A principios de la década de 1990, muchos de los programas que se requieren en un sistema operativo -como bibliotecas, compiladores, editores de texto, el Shell Unix, y un sistema de ventanas- ya se encontraban en operación. Sin embargo otros elementos como los controladores de dispositivos y los servicios estaban incompletos.

Linus Torvalds ha declarado que si el núcleo de GNU hubiera estado disponible en el momento (1991), no se habría decidido a escribir su propio núcleo. Aunque no fue liberado hasta 1992 debido a complicaciones legales, el desarrollo de BSD -de los cuales NetBSD, OpenBSD y FreeBSD descienden- es anterior al de Linux. Torvalds también ha declarado que si BSD hubiera estado disponible en ese momento, probablemente no habría creado Linux.

En 1991 Torvalds asistía a la Universidad de Helsinki. Usuario de MINIX y de los programas provenientes de GNU, se mostraba interesado por los sistemas operativos. Comenzó a trabajar en su propio núcleo en ese año, frustrado por la concesión de licencias que utilizaba MINIX, que en ese momento se limitaba a uso educativo.

El núcleo Linux maduró hasta superar a los otros núcleos en desarrollo. Las aplicaciones GNU también reemplazaron todos los componentes de MINIX, porque era ventajoso utilizar el código libre del proyecto GNU con el nuevo sistema operativo. El código GNU con licencia bajo la GPL puede ser reutilizado en otros programas de computadora, siempre y cuando también se liberen bajo la misma licencia o una licencia compatible. Torvalds inició un cambio de su licencia original, que prohibía la redistribución comercial a la GPL. Los desarrolladores de ambas partes trabajaron para integrar com-

[40] Top500.org informó, en su lista de noviembre de 2017 -y así ha continuado hasta ahora-, que las 500 supercomputadoras más potentes del mundo utilizan Linux.

ponentes de GNU con el núcleo Linux, consiguiendo un sistema operativo completamente funcional.

Para darnos una idea del frenético crecimiento del Kernel de Linux, por ejemplo, en la versión 4.10 se añadieron 632,782 líneas de código nuevo y en el Kernel 4.12 se añadieron más 1.2 millones de líneas de código nuevas, teniendo un total de 24,170,860 líneas de código. El número de desarrolladores involucrados fue de 1821 colaboradores y 220 empleados hicieron un promedio de 231 cambios por día, casi 10 cambios por hora, diariamente se añadieron casi 20 mil líneas de código, y casi 800 líneas por hora en dicha versión.

Hay que precisar que, si bien el código alojado en el repositorio del Kernel es cuantioso, sólo una pequeña parte del mismo afectará a nuestras propias instalaciones de GNU/Linux, pues gran parte del código fuente es específico para cada una de las (múltiples) arquitecturas de Hardware compatibles con Linux.

De hecho, a principios de 2018, Greg Kroah-Hartman (responsable de mantenimiento del código), afirmó que "un portátil promedio usa alrededor de 2 millones de líneas de código del Kernel para funcionar correctamente", cuando en aquel momento, el Kernel completo ya contaba con 25 millones de líneas de código (que ya han aumentado a más de 28 millones en la versión 5.8).

GNU/Linux puede funcionar tanto en entorno gráfico como en modo consola. La consola es común en distribuciones para servidores, mientras que la interfaz gráfica está orientada al usuario final del hogar como empresarial. Así mismo, también existen los entornos de escritorio, que son un conjunto de programas conformado por ventanas, íconos y muchas aplicaciones que facilitan el uso de la computadora. Los entornos de escritorio más populares en GNU/Linux son: GNOME, KDE, LXQt, LXDE, Xfce, Unity, MATE, Cinnamon, Pantheon, Deepin, Budgie, PIXEL, Enlightenment, Trinity, Moksha, Ukui, entre muchos otros.

¿Qué es lo que está llevando a la gente a probar distribuciones de GNU/Linux y a utilizarlas como sistema operativo principal en sus equipos de cómputo? A continuación, vamos a exponer una lista con las razones por las que deberías probar una distribución de GNU/Linux -ya que es una sabia elección- como sistema operativo principal en tu equipo de cómputo:

Software Libre y Código Abierto muchos usuarios de internet no conocen el significado principal del Software libre ni del código abierto. Software libre son esos programas que se automanifiestan, por parte de sus autores, que puede ser copiado, modificado y redistribuido con o sin cambios o mejoras. El concepto de código abierto, es el Software desarrollado y distribuido libremente. Tiene beneficios prácticos ya que si alguien tiene una idea o piensa que puede mejorar el código puede modificarlo sin problemas.

Seguridad no descubrimos el agua tibia diciendo que el sistema operativo de Microsoft es el más atacado por virus y Malware y además, se han descubierto varios virus para Mac OS, unos que llevan ocultos mucho tiempo. Pero con GNU/Linux eso no pasa, ya que es un sistema suficientemente seguro y que no tenemos muchos registros de ataques a esta plataforma.

Aunque hay compañías Linuxeras, como Oracle, Novell, Canonical, Red Hat o SUSE, donde el grueso de distribuciones y Software Linux está mantenido por usuarios y colectivos sin ánimo de lucro. A diferencia de Microsoft y Windows, detrás de Linux no es habitual encontrarnos con una empresa con intereses empresariales, de manera que es más fácil evitar problemas de tipo legal o violaciones de nuestra privacidad o seguridad por parte de quienes han programado esa aplicación o versión de GNU/Linux que usamos. Un ejemplo es la recopilación de datos de uso. A diferencia de los sistemas operativos comerciales, en GNU/Linux no es habitual toparse con este problema.

Es Gratis aunque Mac OS X también es gratuito, está pensado para funcionar solamente en equipos de cómputo Apple. En cuanto a Windows, a pesar de la tendencia, sigue siendo de pago, a pesar de las muchas ofertas que hizo para cambiar de Windows 7 a Windows 10.

Si adquieres una computadora nueva con Windows, el precio incluye la licencia de compra. Por otro lado, todo el mundo sabe que los sistemas operativos de GNU/Linux son totalmente gratuitos y puedes instalarlos en cualquier equipo de cómputo. Las distribuciones más populares puedes descargarlas desde sus páginas oficiales e instalarlas las veces que quieras y en el número de equipos de cómputo que necesites. Además, no tendremos que pagar por utilizar el Software, sin embargo, podremos donar lo que nos plazca al proyecto para que sigan mejorándolo.

Fácil de Utilizar muchos de nosotros hemos utilizado un sistema operativo basado en GNU/Linux y no lo sabíamos. Aeropuertos, estaciones de tren, sistemas de gestión empresarial y ahora en el espacio con SpaceX, etc. Muchos de estos sistemas están basados en GNU/Linux.

Una de las barreras que durante años ha evitado a muchos usar Linux es su complejidad. O al menos lo era cuando la mayoría de tareas debías hacerlas desde la línea de comandos.

En la actualidad, distribuciones GNU/Linux como Ubuntu, Mint, Manjaro, Debian u OpenSUSE ofrecen una interfaz similar a Windows y con todas las herramientas y aplicaciones necesarias para empezar a disfrutar desde el primer día.

Si necesitas un nuevo Software, la mayoría de distribuciones cuentan con su propia tienda de aplicaciones o herramienta de gestión de aplicaciones. Todo está pensado para que cualquiera pueda manejarse sin problemas.

Está claro que existen versiones de GNU/Linux complejas, pero están enfocadas a un público muy concreto. Las distribuciones domésticas cumplen con creces con los requisitos de usuarios amateurs o recién llegados.

Versatilidad configurar un sistema a nuestro gusto, en Windows o en Mac OS X, es algo realmente difícil, pero con los sistemas operativos basados en GNU/Linux se puede tener un sistema operativo totalmente único y totalmente personalizable.

La naturaleza de GNU/Linux y su filosofía de código abierto y libre hace posible que contemos con cientos de versiones diferentes. Esto implica que podamos elegir una versión de GNU/Linux, o distribución, en función de para qué la queremos. ¿Para educación? ¿Para niños? ¿Para uso doméstico? ¿Para gestión de redes? ¿Para temas de seguridad? ¿Para reciclar un PC antiguo? Incluso las hay para arreglar problemas de Windows.

Esta variedad significa que no sólo podemos emplear GNU/Linux en una computadora doméstica. Los ejemplos más claros son Raspberry Pi, Jetson Nano, Pine64 y Arduino[41], son soluciones baratas y diminutas para montar tu propia computadora personal, tu centro multimedia o cualquier artilugio electrónico que desees diseñar. Y para hacerlo funcionar, cuentas con varias distribuciones Linux enfocadas a dicho Hardware.

[41] Son ordenadores del tamaño de una tarjeta de crédito que se conectan a un televisor, un teclado y ratón. Es una placa que soporta varios componentes necesarios en un ordenador común y cuyo precio inicial es de 15 dólares.

Usar GNU/Linux significa que puedes cambiar cualquier elemento de tu sistema operativo. Me refiero a ir más allá de los programas y aplicaciones por defecto. GNU/Linux cuenta con diferentes escritorios y gestores de ventanas, de manera que podemos elegir el que queramos, algo que permiten muchas distribuciones GNU/Linux. Mientras que Windows cuenta con un escritorio por defecto, en GNU/Linux podemos elegir entre: GNOME, KDE, LXQt, LXDE, Xfce, Unity, MATE, Cinnamon, Pantheon, Deepin, Budgie, PIXEL, Enlightenment, Trinity, Moksha, Ukui, etc. En la variedad está el gusto.

Además, cualquier configuración o elemento del sistema operativo es susceptible de ser alterado[42]. La única limitación es que seamos capaces o tengamos los conocimientos adecuados. Pero siempre podemos encontrar en internet un tutorial donde nos explique cómo hacerlo.

Existen distribuciones de Linux de tamaño muy reducido, por ejemplo: BasicLinux ocupa 2.8 MB, requiere un procesador 386 y 3 MB de RAM y cuenta con el escritorio gráfico JWM, Nanolinux ocupa 14 MB, utiliza SLWM como escritorio y cuenta con navegador, procesador de texto, hoja de cálculo, cliente IRC, etc.

Actualizaciones del Sistema Operativo hablando de actualizaciones, sus aplicaciones se actualizan prácticamente al día, en cuanto el desarrollador lanza dicha actualización. Por lo que siempre podemos tener nuestros programas y aplicaciones actualizadas.

Además para los usuarios que así lo requieran existen versiones de soporte a largo plazo (Long-Term Support , LTS) normalmente se asocia con una aplicación o un sistema operativo para el que obtendremos seguridad, mantenimiento y (a veces) actualizaciones de funciones durante un período de tiempo más largo.

Las versiones LTS se consideran las versiones más estables que se someten a pruebas exhaustivas y en su mayoría incluyen años de mejoras en el camino.

[42] BlendOS este prometedor sistema operativo, introduce muchas novedades, empezando porque ahora soporta distintas distribuciones: Arch (el principal), AlmaLinux, Crystal Linux, Debian, Fedora, Kali Linux, Neurodebian Bookworm, Rocky Linux y Ubuntu.

Además de estar disponible en siete entornos gráficos, y que se puede cambiar entre ellos con un sencillo comando. Los entornos en los que está son GNOME, KDE (Plasma), Cinnamon, Xfce, LXQt, MATE y Deepin. El comando para ir cambiando entre los escritorios disponibles es: *sudo system track*. Esta distribución es inmutable, por lo que es difícil que subir de versión estropee algo. Básicamente son imágenes completas a las que se le pueden hacer pequeños retoques, como instalar nuevo software. Pero casi todo va por contenedores.

Es importante tener en cuenta que una versión de Software LTS no implica necesariamente actualizaciones de funciones a menos que haya una versión más reciente de LTS. Sin embargo, obtendrá las correcciones de errores y las correcciones de seguridad necesarias en las actualizaciones de una versión de Soporte a largo plazo.

Se recomienda una versión LTS para consumidores, negocios y empresas listos para la producción porque obtiene años de soporte de Software y sin cambios que rompan el sistema con las actualizaciones. Si observamos una versión que no es LTS para cualquier Software, generalmente es la versión más avanzada con nuevas funciones y un período corto de soporte (por ejemplo, 6-9 meses) en comparación con 3-5 años de soporte en un LTS.

Tiendas de Aplicaciones lo mejor de las distribuciones de GNU/Linux es que tienen una característica en común, sus tiendas de aplicaciones. Ya que vamos a poder instalar cualquier tipo de programa que necesitemos con un Click. Recordamos que esto es algo que Windows está intentando con su propia tienda de aplicaciones, pero no están teniendo muy buenos resultados.

Compatibilidad muchos han experimentado problemas a la hora de actualizar sus sistemas operativos con los programas que tenían instalados. Pero eso con GNU/Linux, no pasa, ya que todas sus actualizaciones tienen retrocompatibilidad a largo plazo dentro de su distribución.

Hoy en día la mayoría de aplicaciones y servicios Online cuentan con versión compatible para cualquier sistema operativo. Siendo más fácil crear una aplicación multiplataforma, por lo que GNU/Linux cuenta con un catálogo de Software que poco o nada tiene que envidiar a Windows o Mac OS X.

En el catálogo destacan las aplicaciones gratuitas y de código abierto, pero también surgen proyectos comerciales, y en la lista se incluyen los juegos, cada vez más presentes en GNU/Linux.

Seguramente hay algún Software no disponible en GNU/Linux, pero es más que probable que encontremos una alternativa o, en su defecto, que podamos ejecutarlo mediante Wine o empleando máquinas virtuales como KVM/QEMU o VirtualBox.

En cuanto al Hardware, la comunidad GNU/Linux ha avanzado mucho en la creación de controladores o Drivers para emplear cualquier dispositivo o componente en GNU/Linux. Podemos encontrarnos con alguna excepción, pero la mayoría de dispositivos cuentan con un controlador compatible por

defecto.

Está en Todas Partes GNU/Linux está presente en la infraestructura de grandes empresas como Amazon, Facebook, Netflix, NASA, SpaceX, el gran colisionador de hadrones o IBM y en el año 2021 llegó a Marte en el sistema operativo del helicóptero que acompaña al rover Perseverance, etc. A nivel de usuario, muchos dispositivos emplean este sistema operativo, bien en alguna de sus versiones o a través de Android, que salvando las distancias, todavía conserva gran parte de su origen Linuxero. Por otro lado, las quinientas principales supercomputadoras emplean Linux como sistema operativo, ya que permite trabajar en todo tipo de entornos y situaciones.

Las grandes empresas de internet hace años que vieron en GNU/Linux una gran oportunidad, y si bien a nivel usuario doméstico no está tan extendido, nunca había sido tan fácil dar el paso. Para hacernos una idea, sólo hay que ver la lista de empresas que apoyan a GNU/Linux a través de The Linux Foundation. Una de las más recientes, la propia Microsoft.

La Comunidad GNU/Linux finalmente, hay que hablar de la fabulosa comunidad de GNU/Linux. Podemos preguntar lo que queramos en sus foros, cambiar el código, enviar tus programas, sin problemas. ¿Trabas en la configuración? Te lo solucionan sin preocupación, ¿consejos sobre Software? Hay cientos de hilos con soluciones. Y nosotros ponemos nuestro granito de arena con este trabajo.

Programas de Windows y macOS en Linux A medida que va pasando el tiempo, las diferencias entre los sistemas operativos se van volviendo irrelevantes. Máquinas virtuales, contenedores y otras tecnologías permiten que podamos utilizar cada día más títulos de nuestros programas preferidos aunque no tenga versión para nuestro sistema operativo.

Wine, la herramienta que actúa como un intérprete entre el núcleo Linux y las aplicaciones Windows ya lleva mucho tiempo entre nosotros. Desde hace poco tiempo, también tenemos una herramienta para los programas de macOS.

Wine para Aplicaciones de Windows Nació inicialmente como un proyecto que buscaba crear un emulador de Windows. Su acrónimo era inicialmente «WINdows Emulator», aunque viendo su evolución, y la forma de funcionar,

este acrónimo fue actualizado por «Wine Is Not an Emulator». Y es que en realidad no es un emulador, sino que este programa está formado por un cargador de programas binarios junto a un conjunto de herramientas de desarrollo que permiten portar en tiempo real el código de las aplicaciones de Windows a Unix. Además, trae por defecto una gran cantidad de bibliotecas y librerías de manera que no tengamos problemas de dependencias.

Principales Características este programa es capaz de ejecutar sin problemas cualquier programa diseñado para cualquier versión de Windows, desde la 3.x hasta Windows 10. Eso sí, solo es compatible con programas Win32 (tanto de 32 bits como de 64 bits), por lo que no vamos a poder ejecutar las apps UWP de la Microsoft Store, al menos por ahora.

Entre toda la variedad de librerías, bibliotecas y recursos, podemos encontrarnos con prácticamente todas las bibliotecas de interrupciones para programas, lo que permite hacer llamadas INT en tiempo real. De esta manera, los programas no saben que se están ejecutando en un sistema operativo que no es Windows, simplemente se ejecutan. Y lo hacen igual que en él. Si algún programa, o juego, tiene dependencias especiales (por ejemplo, una DLL concreta) podemos añadirla fácilmente a Wine. Todas las librerías se encuentran dentro del directorio «~/.wine/drive_c/windows/system32», que equivale al directorio System32 de Windows.

Por supuesto, Wine tiene soporte para una gran cantidad de recursos gráficos. Los programas se pueden dibujar tanto en una interfaz gráfica X11 (el escritorio) como desde cualquier terminal X. Es compatible con las tecnologías OpenGL, DirectX y cuenta con soporte total para GDI (y parcial para GDI32). También permite y gestionar varias ventanas a la vez (del mismo programa, o de diferentes) y es compatible con los temas msstyle de Windows.

También es compatible con los controladores de sonido de Windows, y tiene acceso a los puertos del PC, al Winsock TCP/IP y hasta a los escáneres.

¿Qué Programas y Juegos Puedo Ejecutar con Wine? por desgracia, a pesar de tener una gran compatibilidad, Wine no es capaz de ejecutar el 100% de los programas y juegos de Windows en Linux. Y algunos, aunque se pueden ejecutar, no funcionan del todo bien. Para saber si un programa se puede ejecutar, o no, en Linux, podemos buscarlo en la red del proyecto. Allí vamos a encontrar una gran base de datos que nos va a per-

mitir saber si un programa funciona va a funcionar, si no lo hace, o qué tal lo hace.

Además de poder buscar manualmente cualquier programa o juego, también vamos a encontrar una lista con los Top-10 que mejor funcionan. Los juegos «Platino» son los que funcionan de manera idéntica en Windows que en Linux, los «Oro» los que funcionan bien, pero requieren de alguna configuración especial y los «Plata», los que funcionan, pero tienen pequeños problemas. Los programas o juegos «Bronce» o «Basura» son los que no funcionan.

Saca Todo el Partido a Wine con Estos Programas Wine, al final, es la parte más importante para poder usar programas de Windows en Linux. Sin embargo, su configuración, sobre todo para los programas que no tienen una clasificación de platino, puede ser algo tediosa. Por suerte, existen programas que, aunque se basan igualmente en Wine, nos ayudan a configurar cada uno de estos programas de manera automática para que nosotros no tengamos que hacer nada más.

La instalación y configuración de los programas y juegos de Windows para usarlos en Linux es lo peor. Si no tenemos muchos conocimientos podemos perder mucho tiempo y, además, no conseguiremos que todo funcione del todo bien. Aquí es donde entra en juego *PlayOnLinux*. Este programa, gratuito y de código abierto, busca ayudarnos con la instalación y configuración de los programas y juegos para hacerlos funcionar en este sistema operativo.

PlayOnLinux nos ofrece una completa base de datos de programas con sus correspondientes configuraciones óptimas de manera que nosotros solo tengamos que seleccionar el programa que queremos, cargarle su instalador y dejar que este complete el proceso de puesta en marcha. Nada más. Cuando acabe la instalación ya podremos abrir el programa o juego y empezar a usarlo.

Podemos descargar esta herramienta de forma totalmente gratuita desde su página Web, o desde una termina:

```
# apt install playonlinux
```

Descargar e Instalar Wine hay muchas formas de instalar Wine en Linux. Sus desarrolladores tienen binarios específicos para cada distribución, así como unos completos repositorios desde los que vamos a poder descargar y actualizar el programa desde terminal:

```
# apt install wine
```

WINE no es una aplicación que se inicia por sí sola. Es un backend que se invoca cuando se inicia una aplicación de Windows. Lo más probable es que su primera interacción con WINE ocurra cuando inicie el instalador de una aplicación de Windows.

Ejecutar e Instalar Programas Windows una vez instalado, Wine se ejecutará al hacer doble clic sobre cualquier archivo .EXE. Además, te permitirá instalar programas, como si estuvieras en Windows y pondrá los accesos directos en el menú principal bajo la categoría «Wine».

A pesar de lo que mucha gente cree, Wine sirve no sólo para correr aplicaciones «sencillas» de Windows, sino incluso juegos complejos. Es más, está demostrado que terribles juegazos como Sim 3, Half Life 2, Command & Conquer 3, Star Wars: Jedi Knight, o importantes suites como Microsoft Office funcionan a la perfección.

Darling para Aplicaciones de macOS cumple una función similar a la de Wine con los programas de Windows, solo que no tiene ningún complejo en definirse como un emulador. Lo que hace es actuar como un traductor que permite ejecutar los programas de macOS usando los recursos de Linux. El nombre Darling (Querida) es la primera parte del nombre del núcleo de macOS (Darwin) y las primeras 3 letras de Linux. Supongo que la G final es para construir una palabra fácil de memorizar.

Hay que decir que a los desarrolladores de Darling la cosa les resulta más fácil que a los de Wine. No tienen que hacer ingeniería inversa ni reinventar nada dado que se basan en las partes de Darwin que están bajo licencias abiertas. El propio Darling se distribuye bajo la licencia GPL.

Iniciando Darling el programa no tiene interfaz gráfica. Lo ponemos en marcha desde la terminal con el comando:

```
$ darling shell
```

Al escribirlo, Darling creará un directorio raíz virtual o se conectará con uno existente. Además cargará los módulos del núcleo y construirá el sistema de archivos virtual donde ejecutaremos los programas.

Desde la línea de comandos podemos acceder a dos tipos de sistemas de archivos: el tradicional de macOS que incluye los directorios de nivel superior como */Applications*, */Users* y */System* entre otros. Por otro lado, el del sistema operativo anfitrión lo hallamos en una partición denominada */Volumes/SystemRoot*

Podemos verificar el núcleo con el siguiente comando:

```
$ uname
```

y averiguar la versión de macOS con:

```
$ sw_vers
```

salimos de la terminal con

```
$ exit
```

y apagamos el contenedor con:

```
$ darling shutdown
```

Instalación de Programas Si estás usando Linux en arranque dual con macOS y quieres ejecutar alguno de los programas que tienes instalado en la partición de Mac, puedes hacerlo con el comando:

```
$ /Volumes/SystemRoot/run/media/usuario/Macintosh HD
/Applications/nombre_app.app)
```

Muchos programas para macOS se distribuyen en formato .dmg. Para instalarlos en Darling hacemos:

```
Darling [~]$ hdiutil attach Downloads/aplicación.dmg /Vol-
umes/aplicacion
Darling [~]$ cp -r /Volumes/aplicación/aplicación.app /Ap-
plications/
```

En el caso de aplicaciones almacenadas en archivos comprimidos, lo descomprimimos y copiamos en la carpeta */Applications*. Lo mismo con aplicaciones previamente descargadas de la tienda de aplicaciones.

Por último nos quedan las aplicaciones *.pkg*, el formato de paquete nativo de macOS. Este formato implica ejecutar Scripts durante la instalación. Para poder usarlos debemos hacer:

```
Darling [~]$ installer -pkg aplicación.pkg -target /
```

Podemos desinstalar los programas con:

```
Darling [~]$ uninstaller nombre_del_paquete
```

Debemos entender que si bien Darling funciona muy bien con aplicaciones para la línea de comandos, solo tiene funcionalidades muy limitadas para las que necesitan una interfaz gráfica.

Instalación de Darling Si utilizas Debian o derivados, la instalación de Darling no tiene mayor problema. Solo tienes que escribir los comandos:

```
# apt install gdebi
# gdebi darling-dkms_X.X.X.testing_amd64.deb
# gdebi darling_X.X.X.testing_amd64.deb
```

reemplaza las X por el número de versión de los paquetes que descargarás o bien se puede descargar los archivos fuentes del proyecto para su compilación e instalación.

Aprender a Usar Linux Existen diversos sitios Web que están enfocados a explorar detalladamente cada distribución actual o antigua, a un nivel técnico acompañado de grandes y útiles análisis técnicos sobre los mismos, lo que facilita el aprendizaje puntual sobre qué distribución usar o empezar a usar sin tanta incertidumbre, algunos de estos lugares son:

- ArchiveOS https://archiveos.org
- Distro Chooser https://distrochooser.de/es/
- Distro Watch https://distrowatch.com
- Linux Distribution List https://lwn.net/Distributions/

¿Qué otros sabores de GNU/Linux hay?

https://upload.wikimedia.org/wikipedia/commons/1/1b/Linux_Distribution_Timeline.svg

Existen distintas distribuciones de GNU/Linux[43] para instalar, una de las más ampliamente usadas es Debian GNU/Linux[44] y sus derivadas como Ubuntu. La comunidad de GNU/Linux te apoya para obtener, instalar y que de una vez por todas puedas usar GNU/Linux en tu computadora.

Puedes conocer y descargar las diferentes distribuciones desde:

https://es.wikipedia.org/wiki/Anexo:Distribuciones_Linux

https://en.wikipedia.org/wiki/List_of_Linux_distributions

y ver cuál es la que más te conviene:

https://en.wikipedia.org/wiki/Comparison_of_Linux_distributions

o probar alguna versión Live[45]:

https://livecdlist.com/

también las puedes correr como máquina virtual para VirtualBox:

https://www.osboxes.org/

o máquina virtual para QEMU/KVM:

https://docs.openstack.org/image-guide/obtain-images.html

https://github.com/palmercluff/qemu-images

https://bierbaumer.net/qemu/

[43] Una lista de las distribuciones de Linux y su árbol de vida puede verse en la página Web http://futurist.se/gldt/

[44] Algunas de las razones para instalar GNU/Linux Debian están detalladas en su página Web https://www.debian.org/intro/why_debian.es.html

[45] Linux es uno de los sistemas operativos pioneros en ejecutar de forma autónoma o sin instalar en la computadora, existen diferentes distribuciones Live -descargables para formato CD, DVD, USB- de sistemas operativos y múltiples aplicaciones almacenados en un medio extraíble, que pueden ejecutarse directamente en una computadora, estos se descargan de la Web generalmente en formato ISO.

por otro lado, existen diferentes servicios Web que permiten instalar, configurar y usar cientos de sistemas operativos Linux y Unix desde el navegador, una muestra de estos proyectos son:

Distrotest https://distrotest.net
JSLinux https://bellard.org/jslinux
OnWorks https://www.onworks.net

Ahora, Windows 10 Build 2020 con WSL2[46] (Windows Subsystem for Linux), tiene su propio Kernel de Linux que permite instalar de manera casi nativa diversas distribuciones de GNU/Linux permitiendo tener lo mejor de ambos mundos en un mismo equipo.

En la red existen múltiples sitios especializados y una amplia bibliografía para aprender a usar, administrar y optimizar cada uno de los distintos aspectos de Linux, nosotros hemos seleccionado diversos textos que ponemos a su disposición en:

Sistemas operativos

2.5 Android

Android (véase [6]) es un sistema operativo basado en el núcleo Linux (véase apéndice 11.2). Fue diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tabletas y también para relojes inteligentes, televisores y automóviles. Inicialmente fue desarrollado por Android Inc., empresa que Google respaldó económicamente y más tarde, en 2005, compró. Android fue presentado en 2007 junto a la fundación del Open Handset Alliance (un consorcio de compañías de Hardware, Software y telecomunicaciones) para avanzar en los estándares abiertos de los dispositivos móviles. El primer móvil con el sistema operativo Android fue el HTC Dream y se vendió en octubre de 2008. Android es el sistema operativo móvil (SmartPhone y tabletas) más utilizado del mundo, con una cuota de mercado del 86% al año 2020, muy por encima del 13.9% de iOS.

El éxito del sistema operativo lo ha convertido en objeto de litigios sobre patentes en el marco de las llamadas guerras de patentes entre las empresas de teléfonos inteligentes. Según los documentos secretos filtrados en 2013 y 2014,

[46] https://docs.microsoft.com/en-us/windows/wsl/install-win10

el sistema operativo es uno de los objetivos de las agencias de inteligencia internacionales.

La versión básica de Android es conocida como Android Open Source Project (AOSP). El 25 de junio de 2014 en la Conferencia de Desarrolladores Google I/O, Google mostró una evolución de la marca Android, con el fin de unificar tanto el Hardware como el Software y ampliar mercados. El 17 de mayo de 2017, se presentó Android Go. Una versión más ligera del sistema operativo para ayudar a que la mitad del mundo sin Smartphone consiga uno en menos de cinco años. Incluye versiones especiales de sus aplicaciones donde el consumo de datos se reduce al máximo.

Arquitectura del Sistema Android los componentes principales del sistema operativo de Android[47]:

Aplicaciones: las aplicaciones base incluyen un cliente de correo electrónico, programa de SMS, calendario, mapas, navegador, contactos y otros. Todas las aplicaciones están escritas en lenguaje de programación Java.

Marco de trabajo de aplicaciones: los desarrolladores tienen acceso completo a las mismas API del entorno de trabajo usadas por las aplicaciones base. La arquitectura está diseñada para simplificar la reutilización de componentes; cualquier aplicación puede publicar sus capacidades y cualquier otra aplicación puede luego hacer uso de esas capacidades (sujeto a reglas de seguridad del Framework). Este mismo mecanismo permite que los componentes sean reemplazados por el usuario.

Bibliotecas: Android incluye un conjunto de bibliotecas de C/C++ usadas por varios componentes del sistema. Estas características se exponen a los desarrolladores a través del marco de trabajo de aplicaciones de Android. Algunas son: System C library (implementación biblioteca C estándar), bibliotecas de medios, bibliotecas de gráficos, 3D y SQLite, entre otras.

[47] Android tiene la base de Linux, por ello en cualquier dispositivo que soporte dicho sistema operativo es posible instalar una aplicación para acceder a la terminal de línea de comandos -por ejemplo ConnectBot-, y en ella podemos correr los comandos de BASH como en un sistema GNU/Linux.

Runtime de Android: Android incluye un conjunto de bibliotecas base que proporcionan la mayor parte de las funciones disponibles en las bibliotecas base del lenguaje Java. Cada aplicación Android ejecuta su propio proceso, con su propia instancia de la máquina virtual Dalvik. Dalvik ha sido escrito de forma que un dispositivo puede ejecutar múltiples máquinas virtuales de forma eficiente. Dalvik ejecutaba hasta la versión 5.0 archivos en el formato de ejecutable Dalvik (.dex), el cual está optimizado para memoria mínima. La Máquina Virtual está basada en registros y corre clases compiladas por el compilador de Java que han sido transformadas al formato .dex por la herramienta incluida DX. Desde la versión 5.0 utiliza el ART, que se compila totalmente al momento de instalación de la aplicación.

Personalización muchos conocen a Android como el sistema operativo móvil más personalizable. Pero para los que no lo saben, recordamos que está basado en el núcleo de Linux y que muchos desarrolladores están queriendo llevar Android a un sistema operativo de escritorio.

Núcleo Linux: Android depende de Linux para los servicios base del sistema como seguridad, gestión de memoria, gestión de procesos, pila de red y modelo de controladores. El núcleo también actúa como una capa de abstracción entre el Hardware y el resto del Software.

Android sobre KVM (MicroDroid) En enero de 2021 se anunció por parte de Google que trabajan en MicroDroid, una versión minimalista de Android para máquinas virtuales sobre KVM. No es la primera alternativa a Android, nos encontramos con las capas de personalización Android Go, AOSP o las imágenes GSI. En el caso de MicroDroid, estaríamos ante una limitada imagen de Linux basada en Android, para este proyecto, Google está trabajando en adaptar la máquina virtual de Chrome OS (crosvm), que ya se utiliza para ejecutar aplicaciones de Linux en Chrome OS. De esta forma con MicroDroid podría ejecutar pequeñas máquinas virtuales junto a Android, posiblemente para aplicaciones y uso relacionado con DRM, esta modificación constaría con el mínimo de componentes para iniciar el sistema permitiendo aislar datos entre aplicaciones y sistemas operativos en el mismo dispositivo, así como cambiar instantáneamente entre sistemas operativos.

2.6 Chromebook y Chrome OS

Para entender la razón de ser de los Chromebooks, primero tenemos que entender qué es Chrome OS. Se trata de un sistema operativo creado por Google y diferente a Android. Está basado en el Kernel de Linux, y utiliza Chrome como su interfaz de usuario principal. Esto quiere decir que su aspecto es prácticamente idéntico al de Chrome, pero con algunos añadidos como una barra de tareas, un explorador de archivos y otros elementos presentes en cualquier sistema operativo.

Fue anunciado a mediados del 2009 como un intento de crear un sistema basado en la nube y en aplicaciones Web. Esto hacía que, cuando se estaba conectado a internet se pudieran hacer muchas cosas gracias a herramientas como Google Drive o las aplicaciones de la Chrome Web Store, pero que cuando dejaba de tener internet se limitaba mucho sus funciones.

En cualquier caso, y pese a lo limitado que era en sus primeros años, poco a poco Google lo ha hecho evolucionar. Primero se empezaron a añadir opciones a las aplicaciones de Google para poderse utilizar sin conexión, algo que también benefició a los usuarios que usaran Chrome en otros sistemas operativos.

Pero la evolución más grande fue llegando después. El primer gran paso fue el anuncio de la compatibilidad para ejecutar aplicaciones de Android, y se fue implementando directamente la tienda de aplicaciones Google Play de Android para hacer que la experiencia de instalarlas fuera tan nativa como en Android. Aun así, hay que decir que la llegada de Android a Chrome OS ha sido lenta, y han tardado algunos años en hacer que todo vaya funcionando como debería.

Y a mediados de 2018 se anunció que Google Chrome también podrá utilizar aplicaciones creadas para los sistemas GNU/Linux. Con ello, el catálogo de aplicaciones diseñadas para funcionar sin conexión se multiplica beneficiando a la comunidad de desarrolladores libres, aunque también es de esperar que tarde algunos años en estar todo perfectamente integrado, ya que todavía se están lanzando poco a poco mejoras.

Chrome OS es hoy en día un sistema operativo completo. Tiene lo básico, aplicaciones nativas y compatibilidad con Android, que se une al reproductor de medios, gestor de archivos, configuración de impresoras, etcétera. Además, al igual que el navegador, Chrome OS tiene también una versión libre llamada Chromium OS, que pese a no tener la tecnología nativa de Google sirve para que la comunidad de desarrolladores independientes pueda ayudar a

mejorarlo.

Ahora bien, los Chromebook son equipos de cómputo personales que utilizan como sistema operativo Chrome OS, desarrollado por Google y que, a diferencia de Windows, OS X y Linux, están pensados para utilizarse permanentemente conectados a internet, ya que se basan casi completamente en la nube.

Chromebook Apps también se incluye un reproductor multimedia, y todo se sincroniza permanentemente en la nube. Por ello, si pretendemos utilizar un Chromebook sin conexión a internet, su funcionalidad es más limitada que la de otros equipos de cómputo. De hecho, las aplicaciones se instalan a través de Chrome Web Store, la tienda de aplicaciones integrada en Google Chrome, con lo que algunas de las herramientas más habituales (como Office o Skype, por ejemplo) tendrían que verse reemplazadas por Google Drive y Google Hangouts, aplicaciones nativas de Google.

Chrome Web Store no obstante, también se pueden utilizar de forma local sin recurrir a la red, ya que muchos de los servicios de Google disponen de un modo sin conexión que, una vez volvemos a disponer de internet, se sincronizaran sin problemas.

¿Cómo es un Chromebook? en un Chromebook podemos utilizar dispositivos USB sin problemas, como memorias y discos externos, Webcams, teclados y ratones, y por lo general suelen venir con una cantidad de almacenamiento inferior a lo que estamos acostumbrados (ya que lo que se pretende es que todo esté en la nube, y no en nuestro disco duro local). De hecho, al adquirir uno se nos obsequia con 100 GBytes de espacio en Google Drive.

Igualmente, su precio suele ser bastante asequible (desde 179 dólares o 130 euros) y no requieren de un Hardware potente para funcionar, siendo la ligereza de recursos una de sus mayores bondades. Por su parte, los equipos de cómputo portátiles con Chrome OS son lo que llamamos Chromebook, mientras que si preferimos el formato Mini PC, estaremos ante un Chromebox.

El inicio del sistema es prácticamente instantáneo y todo está listo para funcionar en cuestión de segundos, y dadas sus características, un Chromebook es un equipo ideal para navegar por internet ante todo.

Se accede desde la barra de herramientas en la parte inferior de la pantalla a las aplicaciones que tengamos instaladas, que en realidad se trata de un atajo a las apps que tengamos instaladas en Google Chrome.

Chromebook Integración por supuesto, los Chromebook también son multiusuario, con la ventaja de que con simplemente iniciar sesión con otra cuenta de Gmail todo estará tal y como si lo hubiésemos configurado con ella (aplicaciones, servicios, historial y demás), y por este mismo motivo se complementan a la perfección con otros dispositivos (ya sean equipos de cómputo, Smartphones o Tablets) en los que utilicemos los servicios de Google, gracias a la sincronización en la nube.

Además, los Chromebook también presumen de no necesitar antivirus, pues al almacenarse todo en la nube la seguridad está integrada por defecto y corre por parte de Google.

Microsoft en un Chromebook En el 2020 las empresas Parallels[48] y Google llegaron a un acuerdo para ofrecer a los usuarios la posibilidad de ejecutar aplicaciones Windows en Chrome OS. Ellas aseguran que en Chrome OS la integración será completa: las aplicaciones se ejecutarán cada una en su propia ventana, como las nativas, y no dentro de un Windows virtualizado.

Aunque ninguna de las dos compañías ha ofrecido aún una lista de aplicaciones compatibles con esta función que será lanzada en el 2021, John Solomon (vicepresidente de Chrome OS) ha afirmado que Microsoft Office será una de ellas.

El problema es que, por ahora, estas nuevas funcionalidades no estarán disponibles para todos los usuarios de Chrome OS, sino únicamente para los de Chrome OS Enterprise, la versión empresarial del mismo.

Nota: en últimas fechas han aparecido proyectos que permiten instalar diversas distribuciones de GNU/Linux en los Chromebook, esto es debido a que Google deja de dar soporte a sus equipos después de algunos años de que salieron al mercado, pese a que el equipo es totalmente funcional.

Chrome OS Flex En febrero del 2022, Google anunció su nueva versión de Chrome OS para equipos de cómputo PCs y Macs, la propuesta es Chrome

[48] Empresa (propiedad de Corel desde hace un año) desarrolladora del Software homónimo de virtualización que es especialmente popular entre los usuarios de Mac.

OS Flex y cuya descarga es totalmente gratuita, tiene como propósito atender las necesidades de escuelas y empresas rehusando equipo (procesador Intel o AMD 64 bits, 4 GB RAM, 16 GB de almacenamiento, etc). Esta versión tiene la misma interfaz gráfica y herramientas básicas que se encuentran en Chrome OS; entre ellas el navegador Chrome, se ofrece soporte para sincronización de ajustes y marcadores. Además, si nuestro equipo cumple con las especificaciones básicas, tendremos a nuestra disposición a Google Assistant e integraciones diversas con dispositivos Android.

Es de notar que Chrome OS Flex no tiene soporte para la Play Store o para las aplicaciones de Android y al parecer no hay intención de añadir esta compatibilidad. Tampoco se puede ejecutar Windows en una máquina virtual de Parallels Desktop.

Se puede descargar Chrome OS Flex para crear una unidad USB booteable y la instalación reemplazará al sistema operativo del equipo donde se instale (Mac, Windows o Linux). Pero no está optimizado para sacar provecho de todos los puertos, sensores o accesorios que pueden estar presentes en el equipo. Esto nos proporcionará una experiencia lo más cercana posible a Chrome OS sin comprar un Chromebook pese a sus limitaciones.

2.7 Otros Sistemas Operativos

Sistemas Operativos para PC

1. El sistema operativo OpenKylin 2.0 de China presentado en 2024 se destaca por su capacidad para ejecutar tareas de inteligencia artificial de manera local, sin necesidad de conectarse a la nube. Esta característica no solo mejora la velocidad de procesamiento, sino que también protege mejor la privacidad del usuario, ya que no es necesario enviar datos sensibles a servidores externos (aunque en este caso debemos recordar que se hable de China).

2. Fuchsia OS.- Es un sistema operativo versátil y adaptable esta basado en el microkernel Zircon en desarrollo por parte de Google, está disponible desde un repositorio de Git y está ya siendo usado en los Nest Hub, se espera su uso en la domótica que prepara Google como parte del internet de las cosas.

3. Dahlia OS.- Este sistema operativo combina lo mejor de GNU/Linux y Fuchsia OS es moderno, seguro, liviano y receptivo. Se mantiene

minimalista al incluir solamente las aplicaciones necesarias, pero es posible agregar todos nuestros favoritos de otros sistemas operativos usando aplicaciones Containers y proporciona una tienda para aplicaciones Flutter de terceros.

4. HyperOS.- La nueva estrategia de la firma asiática Xiaomi busca integrar la experiencia de Hombre x Coche x Hogar gracias a HyperConnect. Será la capa que englobará a todos los dispositivos del ecosistema Xiaomi y gracias al nuevo protocolo HyperConnect que sirvira para crear una "red dinámica en tiempo real autónoma entre dispositivos" del ecosistema como Smartphones, tabletas, dispositivos IoT como el aire acondicionado, etc.

5. KataOS.- Es un sistema operativo centrado en la seguridad y los sistemas embebidos que está construido casi enteramente con Rust. No emplea Linux ni Fuchsia, sino el micronúcleo seL4, el cual, según Google, "pone la seguridad al frente y en el centro". Lo que se pretende con este sistema operativo es proporcionar "una plataforma segura verificable que protege la privacidad del usuario porque es lógicamente imposible que las aplicaciones violen las protecciones de seguridad del Hardware incluidas en el kernel, además de que los componentes del sistema son seguros de forma verificable".

6. ToaruOS.- Es un sistema operativo escrito desde cero y provisto con su propio Kernel, cargador de arranque, biblioteca C estándar, administrador de paquetes, componentes de espacio de usuario y una interfaz gráfica con un administrador de ventanas compuesto. Se inició como un proyecto de investigación en la Universidad de Illinois en el 2010 y a partir del 2012 es desarrollado por la comunidad interesada.

7. Essence, es un sistema operativo con su propio Kernel y escritorio construido desde cero por un entusiasta desde 2017 y se destaca por su original escritorio y pila de gráficos que permite dividir ventanas en pestañas, lo que permite trabajar en una ventana con varios programas a la vez y agrupar aplicaciones en ventanas según las tareas a resolver. El administrador de ventanas funciona al nivel del Kernel del sistema operativo y la interfaz se crea utilizando su propia biblioteca gráfica y un motor de Software vectorial que admite efectos animados complejos completamente vectoriales.

8. eComStation.- Seguro que muchos recuerdan el mítico OS/2 de IBM, sistema operativo que perdura con eComStation, derivado de este adaptado al Hardware moderno. A diferencia de otras alternativas de la lista, este no es gratuito y sus precios comienzan desde 145 dólares para la versión doméstica. Muchas aplicaciones libres como Firefox, OpenOffice o VLC han sido portadas a este sistema operativo.

9. Haiku.- BeOS fue un sistema operativo lanzado en el año 1991 con muy buenas intenciones a nivel de optimización e interfaz. Sin embargo, como les sucedió a muchos otros, terminó sucumbiendo en este complicado mercado. Su legado ha sido continuado por Haiku, un sistema de código abierto que lleva ya años en desarrollo.

10. ReactOS.- Es una alternativa a la arquitectura Windows NT de Microsoft totalmente abierta que no utiliza ningún tipo de código propietario. No obstante, es compatible con muchos de los controladores y aplicaciones de Windows. Como punto negativo, su desarrollo no es tan rápido como muchos esperarían en un entorno tan cambiante como este.

11. FreeDOS.- Alternativa libre a DOS cuyo desarrollo sigue activo en estos momentos. Se trata de un entorno bastante estable, pero que carece de interfaz gráfica o multitarea. Es compatible a todos los niveles con MS-DOS y sus programas.

12. Solaris.- El sucesor de SunOS, de Sun Microsystems, empezó como una distribución propietaria de UNIX, pero en 2005 fue liberado como OpenSolaris. Más tarde, Oracle compró Sun y le cambió el nombre a Oracle Solaris.

13. Illumos.- Basado en Open Solaris, este proyecto nació por parte de algunos de los ingenieros originales del sistema. En realidad, busca ser una base para crear distribuciones de este sistema operativo. OpenIndiana es una de las más conocidas y utilizadas.

14. DexOS.- Un sistema operativo de 32 Bits escrito para la arquitectura x86 en lenguaje ensamblador. Está diseñado para programadores que desean tener acceso directo al Hardware (incluyendo CPU y gráficos) con un código bien comentado y documentado.

15. Syllable.- Sistema operativo nacido como fork de AtheOS, un clon de AmigaOS, aunque comparte mucho código con Linux. No tiene demasiada utilidad para los usuarios domésticos, aunque es compatible con arquitecturas x86.

16. AROS Research Operating System.- Es otro sistema que implementa en código abierto las APIs de AmigaOS, con cuyos ejecutables es compatible a nivel binario en procesadores de 68k, además de ser compatible a nivel de código con otras arquitecturas como x86 para la que se ofrece de manera nativa. Es portable y puede correr hospedado en Windows, Linux y FreeBSD.

17. MenuetOS.- Llamado también como MeOS, su característica más destacada es que está programado completamente en lenguaje ensamblador. Está diseñado para funcionar en equipos muy básicos aunque soporta hasta 32 GigaBytes de RAM. Con decir que el sistema cabe en un disquete de 1.44 Megabytes, está dicho todo. Aún así se las arregla para incluir un escritorio gráfico y controladores para teclados, video, audio, USB o impresoras.

18. Visopsys.- Se trara de un sistema gratuito y libre bajo GPL que ha estado en desarrollo desde 1997, como hobby de un solo programador, Andy McLaughlin. Soporta arquitecturas x86, está escrito en C y ensamblador y no se basa en ningún sistema preexistente, si bien utiliza código del kernel Linux, ofrece herramientas comunes de GNU y parte de la interfaz gráfica de usuario como los iconos, resultaran familiares a los usuarios de KDE Plasma.

19. mOS.- Sistema operativo usado en centros de datos y para cómputo de alto rendimiento (High Performance Computing HPC), se basa en el Kernel de Linux pero tiene su propio núcleo ligero LWK, el Kernel gestiona un pequeño número de núcleos de la CPU para asegurarse la compatibilidad y el LWK Kernel gestiona el resto del sistema.

20. KolibriOS.- Es un pequeño sistema operativo poderoso y rápido para PCs. Solamente requiere unos pocos megas de espacio en disco y 8 MB de RAM para funcionar, además de incluir varias aplicaciones básicas.

21. SerenityOS es un sistema operativo Unix con aspecto de Windows de los 90s creado por un único programador como un proyecto terapéutico

y está pensado para equipos X86 de escritorio.

22. BlendOS este prometedor sistema operativo Linux, introduce muchas novedades, empezando porque ahora soporta distintas distribuciones: Arch (el principal), AlmaLinux, Crystal Linux, Debian, Fedora, Kali Linux, Neurodebian Bookworm, Rocky Linux y Ubuntu. Además de estar disponible en siete entornos gráficos, y que se puede cambiar entre ellos con un sencillo comando. Los entornos en los que está son GNOME, KDE (Plasma), Cinnamon, Xfce, LXQt, MATE y Deepin. Esta distribución es inmutable, por lo que es difícil que subir de versión estropee algo. Básicamente son imágenes completas a las que se le pueden hacer pequeños retoques, como instalar nuevo Software, pero casi todo va por contenedores.

Sistemas Operativos para móviles

1. PinePhone.- Usa un sistema operativo basado en sistemas operativos de código abierto impulsado por la comunidad Linux, ha sido portado a 16 diferentes distribuciones de Linux y 7 diferentes interfaces gráficas de usuario como: Mobian, Manjaro con interfaz plasma, Ubuntu Touch, postmarketOS, LuneOS, Nemo Mobile, Maemo Leste, Tizen, entre otros. Además la compañía Pine64 es el segundo fabricante de teléfonos (después de OpenMoko) que ofrece el arranque desde una tarjeta microSD, que permite a los usuarios probar múltiples sistemas operativos, antes de instalarse en la memoria Flash interna.

2. HarmonyOS.- Sistema operativo desarrollado por Huawei para reemplazar a Android en sus equipos, es un sistema operativo similar a la idea de Fuchsia OS, con la idea que pueda instalarse tanto en un ordenador, como en un teléfono, tableta, relojes, como en un coche conectado, en donde todos estos dispositivos se conecten entre sí con una sola cuenta, dando así un paso hacia adelante en la utopía de la convergencia.

3. PostmarketOS.- Sistema operativo de Software libre y código abierto en desarrollo principalmente para teléfonos inteligentes y tabletas -es una idea genial, la persecución de tener Linux en los dispositivos Smartphone, como otra alternativa a los sistemas Android e iOS-, haciéndose

las primeras pruebas en teléfonos que ya no tienen uso. Distribución basada en Alpine Linux. Puede usar diferentes interfaces de usuario, por ejemplo Plasma Mobile, Hildon, LuneOS UI, MATE, GNOME 3 y XFCE.

4. Plasma Mobile.- Es un sistema en fase de desarrollo por KDE que permite la convergencia con los usuarios de KDE para escritorio.

5. Lomiri.- Sistema operativo basado en Linux que soporta dos sabores: Ubuntu Touch y Manjaro. Ambos basados en Unity 8 que están en constante desarrollo.

6. Windows Phone.- Sistema operativo móvil desarrollado por Microsoft, como sucesor de Windows Mobile. A diferencia de su predecesor fue enfocado en el mercado de consumo en lugar del mercado empresarial.

7. Symbian OS.- Era un sistema operativo que fue producto de la alianza de varias empresas de telefonía móvil, entre las que se encuentran Nokia, Sony Ericsson y otros, el objetivo de Symbian fue crear un sistema operativo para terminales móviles.

8. BlackBerry OS.- Es un sistema operativo móvil desarrollado por Research In Motion para sus dispositivos BlackBerry.- Es multitarea y tiene soporte para diferentes métodos de entrada adoptados por RIM para su uso en computadoras de mano, particularmente la trackwheel, trackball, touchpad y pantallas táctiles.

9. HP webOS.- Se trata de un sistema operativo multitarea para sistemas embebidos basado en Linux, desarrollado por Palm Inc., ahora es propiedad de Hewlett-Packard Company.

10. GrapheneOS.- Es un sistema operativo móvil centrado en la privacidad y la seguridad con compatibilidad con aplicaciones Android, que está desarrollado como un proyecto de código abierto sin ánimo de lucro. Se centra en la investigación y el desarrollo de tecnología de privacidad y seguridad, incluyendo mejoras sustanciales en el Sandboxing, la mitigación de exploits y el modelo de permisos.

11. Sailfish OS.- Es un Sistema Operativo móvil seguro y optimizado para funcionar en Smartphones y tabletas, y también fácilmente adaptable

a todo tipo de dispositivos integrados y casos de uso. Es el único Sistema Operativo móvil independiente basado en el código abierto, sin ningún vínculo con las grandes corporaciones, respaldado por unos sólidos derechos de propiedad intelectual, que incluyen todos los derechos de propiedad intelectual y marcas comerciales. En resumen, es una plataforma abierta con un modelo de contribución de código abierto activo.

12. Bada.- Fue un sistema operativo para teléfonos móviles desarrollado por Samsung (Bada «océano» o «mar» en coreano). Diseñado para cubrir teléfonos inteligentes de gama alta como gama baja.

3 Seguridad, Privacidad y Vigilancia

Ante el constante aumento -explosivo- en el uso de dispositivos conectados a internet como computadoras personales, Laptops, tabletas y teléfonos celulares, expertos en ciberseguridad advierten un entorno propicio para que prosperen los cibercriminales y que, tanto individuos como empresas, se encuentren expuestos a múltiples amenazas de ciberseguridad.

En la actualidad, aproximadamente la mitad de la población mundial accede de algún modo a internet. Con tantos accesos concurrentes a la red de redes, la posible amenaza de seguridad a los sistemas informáticos crece y se complejiza, a pesar de las diversas y especializadas maneras de contrarrestarlas. Por su propia naturaleza, una conexión a internet hace que tu equipo de cómputo quede expuesto a ataques y pueda ser accesible por otro equipo, llegando a tener acceso a tu información.

¿Por qué?

- En muchas ocasiones, los usuarios no cuentan con la suficiente sensibilización sobre su exposición al riesgo, o bien, no están familiarizados con las herramientas y/o capacitación de sus organizaciones para prevenir y enfrentar amenazas de ciberseguridad.

- Los usuarios de internet a menudo utilizan redes Wi-Fi no seguras y usan dispositivos que no están configurados con los controles de políticas de seguridad básicos, lo cual los vuelve excepcionalmente vulnerables a ataques cibernéticos.

- Es común que los usuarios compartan dispositivos (computadoras, tabletas, teléfonos) para educación, trabajo y esparcimiento aumentando con ello su exposición a amenazas de ciberseguridad.

- Los piratas informáticos eligen como blanco la dependencia, cada vez mayor, de las personas con respecto a las herramientas digitales, además de que más tiempo en línea incrementa la potencial exposición de los usuarios a amenazas de ciberseguridad.

- Un error común es creer que los ciberatacantes utilizan únicamente herramientas muy avanzadas y técnicas para Hackear las computadoras o cuentas de las personas. Los atacantes han aprendido que la forma

más sencilla de robar la información de los usuarios, comprometer sus cuentas o infectar los sistemas es simplemente engañar al usuario para que lo hagan por ellos con una técnica denominada ingeniería social.

- Los piratas informáticos son extremadamente creativos al idear formas de aprovecharse de los usuarios y de la tecnología para acceder a contraseñas, redes y datos, a menudo sirviéndose de herramientas de ingeniería social y de temas y tendencias populares para tentar a los usuarios a tener comportamientos inseguros en línea.

Todo lo anterior, ha creado una enorme superficie de exposición a ataques cibernéticos dirigidos a los usuarios, la red, la computadora portátil, el teléfono inteligente, la tableta, etc. con la intención de cometer delitos informáticos. Por ello estos lineamientos generales de ciberseguridad son sugeridos para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al usuario, contiene recomendaciones sencillas y prácticas para fomentar una buena salud cibernética de los dispositivos utilizados para el trabajo a distancia, educación y diversión; y promover la ciberseguridad entre las personas y sus organizaciones.

La seguridad de la información en la red es más que un problema de protección de datos, y debe estar básicamente orientada en asegurar la información importante de las personas, de las organizaciones y la propiedad intelectual. Los riesgos de la información están presentes cuando confluyen fundamentalmente dos elementos: las amenazas de ataques, y las vulnerabilidades de la tecnología; conceptos íntimamente relacionados donde no es posible ninguna consecuencia sin la presencia conjunta de estos.

3.1 ¿Qué es la Privacidad y por qué es Importante?

Consideramos que la privacidad debería ser un derecho básico y una protección necesaria en la era digital para evitar la victimización y la manipulación. Una sociedad no puede tener libertad sin privacidad. Puede parecer un lujo, pero es importante para el bienestar de una sociedad libre y justa. Muchos gobiernos y empleadores hacen vigilancia[49] activa a sus ciudadanos o empleados para monitorear ideas, discusiones o disensiones no deseadas. Los

[49] ¿Qué es vigilancia? Vigilancia es el seguimiento de las comunicaciones, acciones o movimientos de una persona por un gobierno, empresa, grupo o persona.

¿Cuándo es legal la vigilancia? En general, cuando es selectiva, se basa en indicios suficientes de conducta delictiva y está autorizada por una autoridad estrictamente inde-

infractores son luego procesados o reeducados para alinearse con lo que las autoridades consideran apropiado. Sin el beneficio del anonimato, el deseo de los ciudadanos de expresar sus pensamientos se reprime efectivamente.

En la era digital, la privacidad va más allá del anonimato, al proteger a las personas de la victimización y la manipulación. La sociedad ha adoptado la tecnología para educarse, comunicarse, realizar negocios y formar relaciones. Nuestros puntos de vista y opiniones están fuertemente influenciados por lo que aprendemos de las fuentes de noticias locales, nacionales e internacionales.

Contribuimos en gran medida al panorama digital a través de nuestras acciones y decisiones. Nuestras huellas digitales están en todas partes. Cuentan una historia de a dónde vamos, qué hacemos, quién nos gusta o no, y qué pensamos. Se crean con cada Clic que hacemos y con cada archivo, aplicación y dispositivo que usamos. Cuando esos datos se agregan, pueden proporcionar información tremendamente poderosa sobre una persona o comunidad, lo suficiente como para construir personas complejas y precisas.

Esta información se usa comúnmente para manipular las creencias y comportamientos de las personas. Las compras en línea son un ejemplo perfecto: el Marketing dirigido y la publicidad basada en datos es un gran negocio porque logra que la gente gaste dinero. Todo se reduce a saber lo que las personas hacen, piensan, dicen, consumen y miran[50]. Tener acceso a grandes

pendiente, como un juez.

¿Qué es la vigilancia masiva? La vigilancia masiva indiscriminada es el control de las comunicaciones por internet y telefónicas de un gran número de personas -a veces de países enteros- sin que existan indicios suficientes de conducta delictiva. Este tipo de vigilancia no es legal.

¿Qué datos recogen? Algunos gobiernos almacenan y analizan historiales de navegación, búsquedas en internet, mensajes de correo electrónico, mensajes instantáneos, conversaciones por Webcam y llamadas telefónicas. También reúnen metadatos -datos sobre datos-, como destinatarios de correo electrónico, horas de llamadas y registros de ubicación.

¿Qué hacen con mis datos? Se guardan en grandes centros de datos donde unos algoritmos informáticos pueden hacer búsquedas en ellos y analizarlos. También están a disposición de las autoridades de las agencias de seguridad a través de potentes bases de datos como XKeyscore.

[50]Has notado que si buscas algo en un buscador comercial -como Google, Yahoo, Bing, Ask, Baidu, etc.-, minutos después en tus distintas redes sociales aparecerán mensajes relacionados a tu búsqueda. Esto ocurre porque los buscadores comerciales en cada búsqueda que haces, vídeo o los anuncios que ves o en los que haces Clic comparten tu ubicación, los sitios que visitas, los dispositivos, navegadores y aplicaciones que usas para acceder a los servicios del buscador con fines comerciales.

cantidades de datos privados les brinda a los anunciantes la capacidad de crear mensajes oportunos y significativos que atraigan a las personas a los comportamientos deseados.

Pero si los minoristas pueden hacer que las personas compren cosas que no necesitan, ¿para qué más se pueden usar los datos privados? ¿Qué tal cambiar lo que piensa la gente, a quiénes apoyan, sus opiniones políticas, qué debería convertirse en ley y en qué creer? El uso de información privada se ha aprovechado durante mucho tiempo para promover, vilipendiar o perseguir a diversas religiones, partidos políticos y líderes.

En las últimas décadas, ha cambiado la forma en que los ciudadanos del mundo reciben sus noticias. Los segmentos de noticias y entretenimiento han comenzado a mezclarse, a menudo informando hechos con adornos e historias obstinadas para influir en las opiniones públicas. Cuanta más información privada se conozca, más fácil será influir, convencer, engatusar o amenazar a las personas.

Según informes de Oxford Internet Institute, a pesar de los esfuerzos para combatir la propaganda computacional, el problema ha crecido a gran escala. El mayor crecimiento proviene de propaganda política que es difundida junto con desinformación y noticias basura alrededor de los períodos electorales. Se incrementa el número de campañas políticas a nivel mundial que usan Bots, noticias basura y desinformación para polarizar y manipular a los votantes.

Un velo de privacidad puede proteger tanto los beneficios como los abusos. La tendencia actual es establecer y ampliar los derechos de privacidad en beneficio de los ciudadanos. Esto reduce la victimización, manipulación y explotación digitales al proteger los datos confidenciales y permite actividades que promueven la libertad y la libertad de expresión.

Sin leyes, los gobiernos y las empresas han desarrollado prácticas que aprovechan el poder de recopilar información confidencial y utilizarla en su propio beneficio. Las nuevas leyes de privacidad están cambiando el panorama y muchas empresas éticas reducen sus esfuerzos de cobranza para ser más conservadoras y respetuosas. También muestran flexibilidad en la forma en que tratan, protegen y comparten dichos datos.

Algunos gobiernos y agencias también están reduciendo la recolección, limitando la retención o terminando los programas domésticos que los ciudadanos consideran invasivos. Al mismo tiempo, los organismos encargados

Una opción para nuestra privacidad es usar buscadores que no dejan rastro de nuestras búsquedas como puede ser: DuckDuckGo.

de hacer cumplir la ley quieren conservar la capacidad para detectar e investigar delitos, para proteger la seguridad de los ciudadanos.

También se hace un mal uso de la privacidad. Es la herramienta preferida por quienes cometen delitos y permite que los actos atroces contra otros no se detecten. Puede ocultar actos terribles y permitir una coordinación generalizada entre el fraude, abuso y terror.

Se argumenta que las puertas traseras digitales, las claves maestras y los algoritmos de cifrado que obtienen acceso a los sistemas y la información privada ayudarían en la detección legal de actividades delictivas y en las investigaciones para identificar a los terroristas. Aunque suena como una gran herramienta contra los delincuentes, es una caja de Pandora.

Las puertas traseras y las llaves maestras no limitan el acceso para una investigación específica donde existe una causa probable, sino que permiten una vigilancia generalizada[51] y la recolección de datos de toda una población, incluidos los ciudadanos respetuosos de la ley. Esto viola el derecho de las personas a la privacidad y abre la puerta a la manipulación y el enjuiciamiento político. La capacidad de leer cada texto, correo electrónico, mensaje y conversación en línea para "monitorear" a la población crea un camino claro hacia el abuso. El riesgo de control y explotación es real.

Incluso para aquellos que no tienen ninguna objeción a que su gobierno tenga acceso, debemos considerar el hecho de que tales puertas traseras y

[51] El 5 de junio de 2013, el exanalista de la CIA y de la NSA Edward Snowden decidió revelar la existencia de programas de vigilancia sobre las comunicaciones de millones de ciudadanos de todo el mundo. A través de The Guardian y The Washington Post, supimos que, en nombre de la seguridad y sin ningún control judicial, la NSA y el gobierno británico habían rastreado e-mails, llamadas telefónicas y mensajes encriptados. Empresas como Facebook, Google y Microsoft habían sido obligadas a entregar información de sus clientes por órdenes secretas de la NSA. Esta misma agencia grabó, almacenó y analizó los 'metadatos' de las llamadas y de los mensajes de texto enviados en México, Kenia y Filipinas. Incluso llegaron a espiar el móvil de la canciller alemana Angela Merkel.

Snowden hizo las filtraciones a la prensa desde Hong Kong y actualmente vive en Rusia, donde se le concedió asilo. No puede volver a su país porque está acusado de revelar información clasificada a personas no autorizadas y de robo de propiedad del gobierno federal. Para unos es un héroe y para otros un traidor, gracias a las revelaciones de Snowden la opinión pública es más consciente de su derecho a la privacidad y ha reaccionado oponiéndose al espionaje masivo.

Aunque queda un largo camino para asegurar que los Gobiernos no invadan la vida privada de las personas, los tribunales han declarado ilegales algunos aspectos de estos programas y las empresas tecnológicas han tenido que posicionarse ante un escándalo capaz de dañar seriamente su reputación.

claves maestras serían buscadas por ciberdelincuentes y otros actores del estado-nación. Ningún sistema es infalible. Con el tiempo, los delincuentes encontrarían y utilizarían estas herramientas en detrimento de la comunidad digital mundial. Algunas puertas traseras podrían valer decenas de miles de millones de dólares para el comprador adecuado, ya que podrían desbloquear un poder inimaginable para apoderarse de la riqueza, afectar a la gente, dañar naciones, socavar la independencia y reprimir el pensamiento libre.

Proteger la privacidad no se trata de ocultar información. Se trata de la capacidad de liberarse de influencias no deseadas, de la tiranía y de comunicarse con los demás de formas que desafíen el statu quo. La privacidad protege a las personas, pero también los cimientos de una sociedad libre. La privacidad no es un tema fácil y no existe una solución perfecta. Es una situación dinámica y seguirá cambiando con el sentimiento público.

Todos quieren cierto nivel de discreción, confidencialidad y espacio. Nadie quiere que se expongan sus contraseñas, finanzas familiares, detalles de relaciones personales, historial médico, ubicación, compras y discusiones privadas. Las personas tampoco disfrutan de verse inundadas de Spam, Phishing y llamadas de ventas incesantes. La privacidad no se trata necesariamente de ocultar algo, sino de limitar la información a quienes tienen derecho a saber.

Muy poca privacidad puede socavar la libertad de expresión, la libertad y la denuncia de victimizaciones. También empodera a entidades poderosas para manipular el mundo digital de las personas para coaccionarlas, manipularlas y victimizarlas. Demasiada privacidad puede permitir que los actores criminales prosperen y se escondan de las autoridades. Debe lograrse un equilibrio[52].

[52]Los gobiernos nos enfrentan a un dilema falso: seguridad o libertad. En un estado de derecho, donde las leyes equilibran ambos conceptos, las personas son inocentes hasta que se demuestra lo contrario y tienen derecho a que se respete su vida privada. Por tanto, antes de violar estos derechos, los gobiernos deben de tener indicios de que se está cometiendo un delito. No pueden buscar pruebas aleatoriamente en nuestras comunicaciones privadas antes de que se cometa ese delito.

Varios países dan "carta blanca" a la vigilancia indiscriminada en sus leyes. En Francia se permite interceptar masivamente comunicaciones, retener información durante largos períodos de tiempo y se ha eliminado la autorización judicial previa. También Reino Unido ha introducido en su legislación mayores poderes de espionaje. Polonia ha otorgado poderes de vigilancia incompatibles con respecto a la privacidad a la policía y o otras agencias. Otros países como China o Rusia también vigilan internet con total desprecio a la intimidad de las personas.

Algunos gobiernos y empresas tecnológicas quieren que aceptemos que no tenemos derechos cuando estamos en internet. Que cuando usamos el teléfono o entramos en nuestra cuenta de correo electrónico, todo lo que hacemos o decimos les pertenece. No permitiríamos este grado de intrusión en nuestra vida fuera de internet, así que no debemos permitirlo dentro.

Cuando los gobiernos no protegen los derechos humanos, sólo la acción de la gente común y corriente puede hacer que las cosas cambien y que los responsables de los abusos rindan cuentas. Muchas organizaciones trabajan para que los gobiernos prohíban la vigilancia masiva y el intercambio ilegal de información confidencial. Esta será una larga lucha no exenta de dificultades, pero cuyo impulso va creciendo con el tiempo.

¿Qué son los datos biométricos? en general entenderemos por datos biométricos a las características físicas, fisiológicas, morfológicas, de comportamiento y rasgos de personalidad distintivas de cada persona que permite distinguir ciertas singularidades e identificar al individuo en cuestión.

El uso de datos biométricos no es nuevo e incluso es algo en lo que constantemente se ven envueltos las redes sociales[53], aunque los fines de uso son diversos. Recientemente Texas demandó a Meta, dueña de Facebook, por almacenar millones de estos datos y comercializarla con terceros.

Las Amenazas a los Usuarios en un entorno dinámico de interconectividad, pueden venir de cualquier parte, sea interna o externa, e íntimamente relacionada con el entorno de las organizaciones. Las vulnerabilidades son una debilidad en la tecnología o en los procesos asociados con la información, y como tal, se consideran características propias de los sistemas o de la infraestructura que los soporta.

Las personas o usuarios de internet que emplean las tecnologías para vulnerar los sistemas en la red, robar información y/o infectarlos con comportamientos dudosos, son comúnmente conocidos como *Crackers*.

[53] Por ejemplo en el caso de X antes Twitter, podrá hacerse de tu foto de perfil, así como otros datos que incluyen historial de empleo, educación, preferencias de empleo, capacidades y habilidades, así como búsqueda de trabajo, datos que utilizaría para ofrecer servicios similares a los de Linkedln, "recomendarte potenciales trabajos, compartir con potenciales empleadores cuando solicitas un trabajo, permitir que los empleadores encuentren potenciales candidatos y mostrarte publicidad más relevante".

El término Hacker[54] en el sentido más filosófico tiende a promover una conciencia colectiva de la libertad del conocimiento y la justicia social, por lo que muchas veces se los encuentra en situaciones de activismo (llamado en este caso Hacktivismo) en pos de dicha ideología. Su forma de actuar, por lo general, determina su clasificación en:

- *Hacker* de Sombrero Blanco (White Hat): éticos, expertos en seguridad informática, especializados en realizar test de intrusión y evaluaciones de seguridad.
- *Hacker* de Sombrero Negro (Black Hat): también conocidos como *Crackers*, vulneran los sistemas de información con fines maliciosos.
- *Hacker* de Sombrero Gris (Grey Hat): en ocasiones vulneran la ley, y de forma general no atacan malintencionadamente o con intereses personales, sino que sus motivaciones se relacionan a protestas o desafíos personales.
- *Hacker* de Sombrero Verde (Green Hat): son novatos que pueden evolucionar y buscan convertirse en expertos.
- *Hacker* de Sombrero Azul (Blue Hat): son personas expertas que se les paga para probar Software en busca de errores antes de que éste salga al mercado.

Para una entidad, la fuga de información provocada por el actuar de algunos de estos usuarios de la red, puede ocurrir deliberadamente como resultado de una acción intencional de algún empleado descontento, como consecuencia de un ciberataque, o inadvertidamente, por un colaborador desprevenido víctima de un Software malicioso.

Una de las principales amenazas para los dispositivos tecnológicos utilizados para el trabajo y estudio a distancia es el Malware, también conocido como Software o código malicioso. Éste se define como cualquier programa informático que se coloca de forma oculta en un dispositivo, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo.

[54] Existen algunos otros términos en el ciberespacio, por ejemplo: Newbie, que significa principiante; Lammer, persona que presume tener conocimientos que realmente no posee; Phreaker, Hacker orientado a los sistemas telefónicos; Script Kiddie, quien utiliza programas creados por terceros sin conocer su funcionamiento.

Los tipos más comunes de amenazas de Malware incluyen Virus, gusanos, troyanos, Rootkits y Spyware. Las amenazas de Malware pueden infectar cualquier dispositivo por medio del correo electrónico, los sitios Web, las descargas y el uso compartido de archivos, el Software punto a punto y la mensajería instantánea.

Además, existen amenazas relacionadas con la ingeniería social como el Phishing, Smishing y Vishing, por medio de los cuales los atacantes intentan engañar a las personas para que revelen información confidencial o realicen ciertas acciones, como descargar y ejecutar archivos que parecen ser benignos, pero que en realidad son maliciosos.

3.2 Las Vulnerabilidades y Exposiciones Comunes

De manera global, la última década ha sido testigo del cambio de paradigma en que los atacantes buscan explotar vulnerabilidades dentro de las organizaciones y las infraestructuras de redes. Con el fin de contrarrestar estos ataques, las políticas de seguridad persiguen constantemente aprender de ellos para estar preparados lo mejor posible, y en este sentido, intentar garantizar confianza y tranquilidad a los usuarios de la red, sobre el empleo de sus datos, finanzas y propiedades intelectuales.

Los ataques de seguridad vienen en muchas formas y usan varios puntos de entrada. Cada tipo de ataque viene en varios tipos, ya que generalmente hay más de una forma en que se pueden configurar o camuflar en función de la experiencia, los recursos y la determinación del pirata informático.

Las Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures, CVE[55]) que tienen los distintos sistemas operativos (productos), es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación llamada CVE-ID, descripción de la vulnerabilidad, que versiones del Software están afectadas, posible solución al fallo (si existe) o como confi-

[55] https://www.cvedetails.com/
https://www.cvedetails.com/top-50-products.php
https://thebestvpn.com/vulnerability-alerts/
Hay que notar que en la base de datos se diferencian distintos productos de Windows (como Windows 7.0 u 8.1) pero no se hace lo mismo con los demás productos (por ejemplo para Debian GNU/Linux están los errores desde 1999 a la fecha) con lo que es engañosa la comparación del número vulnerabilidades para un sistema operativo con tantas versiones generadas en dicho tiempo con otro con un tiempo de vida corto.

gurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o Blogs donde se ha hecho pública la vulnerabilidad o se demuestra su explotación. Además suele también mostrarse un enlace directo a la información de la base de datos de vulnerabilidades (https://nvd.nist.gov, https://openssf.org y https://docs.aws.amazon.com/security), en la que pueden conseguirse más detalles de la vulnerabilidad y su valoración.

El mundo está cada vez más interconectado y, como resultado de esto, la exposición a las vulnerabilidades de seguridad también ha aumentado dramáticamente. Las complejidades de mantener las plataformas de cómputo actuales hacen que sea muy difícil para los desarrolladores cubrir cada punto de entrada potencial. En 2019 hubo un promedio de más de 45 vulnerabilidades y exposiciones comunes registradas por día y estas siguen en aumento año con año.

El CVE-ID ofrece una nomenclatura estándar para identificación de la vulnerabilidad de forma inequívoca que es usada en la mayoría de repositorios de vulnerabilidades.

Es definido y es mantenido por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

Por otro lado, como parte de las amplias revelaciones sobre vigilancia masiva filtradas en 2013, 2014 y años posteriores, se descubrió que las agencias de inteligencia estadounidenses y británicas, la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) y el Cuartel General de Comunicaciones del Gobierno (GCHQ, por sus siglas en inglés), respectivamente, tienen acceso a los datos de los usuarios de dispositivos Android. Estas agencias son capaces de leer casi toda la información del teléfono como los SMS, geolocalización, correos, notas o mensajes.

Documentos filtrados en enero de 2014, revelaron que las agencias interceptan información personal a través de internet, redes sociales y aplicaciones populares, como Angry Birds, que recopilan información para temas comerciales y de publicidad. Además, según The Guardian, el GCHQ tiene una wiki con guías de las diferentes aplicaciones y redes de publicidad para saber los diferentes datos que pueden ser interceptados. Una semana después de salir esta información a la luz, el desarrollador finlandés Rovio, anunció que estaba reconsiderando sus relaciones con las distintas plataformas publicitarias y exhortó a la industria en general a hacer lo mismo.

Las informaciones revelaron que las agencias realizan un esfuerzo adi-

cional para interceptar búsquedas en Google Maps desde Android y otros teléfonos inteligentes para recopilar ubicaciones de forma masiva. La NSA y el GCHQ insistieron en que estas actividades cumplen con las leyes nacionales e internacionales, aunque The Guardian afirmó que «las últimas revelaciones podrían sumarse a la creciente preocupación pública acerca de cómo se acumula y utiliza la información, especialmente para aquellos fuera de Estados Unidos de Norte América, que gozan de menos protección en temas de privacidad que los estadounidenses».

3.3 Alfabetismo Digital

Según la organización Common Sense Media, el alfabetismo digital es la capacidad de encontrar, identificar, evaluar y usar la información encontrada en medios digitales de manera efectiva. Básicamente, es la misma definición tradicional de alfabetismo, pero adaptada a la era digital y a fuentes no tradicionales de información.

El anuario del 2016 de la UNESCO en "Alfabetización mediática e informacional para los objetivos de desarrollo sostenible" hace referencia a las "Cinco leyes de la alfabetización mediática e informacional":

1. La información, la comunicación, las bibliotecas, los medios de comunicación, la tecnología, el internet y otras fuentes de información se encuentran en la misma categoría. Ninguna es más relevante que la otra ni debe ser tratada como tal.

2. Cada ciudadano es un creador de información o conocimiento y tiene un mensaje. Todas las personas deben estar facultadas para acceder a nueva información y expresarse.

3. La información, el conocimiento y los mensajes no siempre están exentos de valores o prejuicios. Cualquier conceptualización, uso y aplicación de alfabetismo digital debe presentar este hecho de manera transparente y comprensible para todos los ciudadanos.

4. Todo ciudadano desea conocer y comprender información, conocimientos y mensajes nuevos, así como comunicarse; y sus derechos nunca deben ser comprometidos.

5. El alfabetismo digital es un proceso dinámico de experiencias vividas. Se considera completa cuando incluye conocimientos, habilidades y actitudes, cuando abarca el acceso, la evaluación, el uso, la producción y la comunicación de información, de contenido mediático y tecnológico.

De igual manera, en el anuario de la UNESCO se exponen 10 habilidades que deben desarrollarse para lograr la alfabetización digital, o como lo define el anuario, alfabetización mediática e informacional. Estas habilidades son:

- Interactuar con información referente a los medios y la tecnología.
- Ser capaz de aplicar habilidades técnicas de comunicación de información para procesar la información y producir contenido mediático.
- Utilizar, de manera ética y responsable la información y comunicar su comprensión o conocimiento adquirido a una audiencia o lectores en una forma y medio apropiados.
- Extraer y organizar información y contenidos.
- Evaluar de forma crítica la información y el contenido presentado en los medios y otras fuentes de información, incluyendo medios en línea, en términos de autoridad, credibilidad, propósito y posibles riesgos.
- Localizar y acceder a información de contenido relevante.
- Sintetizar las ideas extraídas del contenido.
- Comprender las condiciones bajo las cuales se pueden cumplir esas ideas o funciones.
- Comprender el papel y las funciones de los medios, incluyendo medios en línea, en la sociedad y su desarrollo.
- Reconocer y articular la necesidad de información y de los medios.

Internet ha sido una herramienta que ha transformado y definido la comunicación en el siglo XXI. A través de sus múltiples interfaces, internet ha tenido éxito, para que tanto individuos como organizaciones se conecten, se comuniquen e intercambien información. Las plataformas tecnológicas y las redes sociales han acelerado la velocidad a través de la cual los usuarios

pueden acceder y recuperar información, simplificando el proceso en el que las noticias se difunden, actualizan e incluso se comunican. Hoy en día, es prácticamente instantáneo darse cuenta de un evento de noticias sin que sea necesariamente comunicado por medios tradicionales como los periódicos o la radio.

La facilidad a través de la cual las personas ahora pueden comunicarse ha traído una sensación de democratización a la libertad de expresión. Transformar la libertad de expresión ha posibilitado nuevas capacidades para crear y editar contenido, generando nuevas oportunidades para el periodismo alternativo; nuevas capacidades de organización y movilización (que apoyan en gran medida otros derechos, como la libertad de asociación); y nuevas posibilidades para innovar y generar desarrollo económico (apoyando los derechos sociales y económicos).

Sin embargo, esta facilidad en el intercambio y la creación de información también presenta desafíos tanto para las organizaciones como para las personas que son usuarias de dichas redes, tanto como fuente, como usuario final. Aunque estos desafíos varían en escala, todos son igualmente significativos. Algunos de los más destacados incluyen el desafío a la calidad superficial de la información, la susceptibilidad a la información errónea y la exposición a ataques cibernéticos. Por lo tanto, la necesidad de mitigar y mantener la integridad de esta información se ha convertido en un área de trabajo creciente para muchas organizaciones públicas y privadas.

En las siguientes secciones se ofrece una variedad de técnicas y mejores prácticas para mitigar y contrarrestar los desafíos mencionados anteriormente. Sin embargo, es importante tener en cuenta, al leer estas recomendaciones, la posición que representas o con la que te asocias. Algunas de las recomendaciones pueden no ser aplicables a una figura pública, como políticos, activistas u otros actores cuyas mejores prácticas en las redes sociales están sujetas a un mayor escrutinio. En este sentido, el ejercicio de los derechos de expresión, reunión y protesta se debe respetar, y debe ser respetado, en el ámbito digital al tiempo que se garanticen prácticas más seguras de internet.

3.4 Amenazas a la Ciberseguridad

La aparición de vulnerabilidades en los sistemas operativos y los métodos de encubrimiento de los atacantes, lo convierten en una práctica en aumento. Algunos de los principales ataques en la red, hacia donde dirigen su mirada

los *Hackers* para vulnerar la seguridad, pueden definirse como:

- Shoulder Surfing: es una técnica mediante la que el ciberdelincuente consigue nuestra información mirando "por encima del hombro" desde una posición cercana, mientras utilizamos los dispositivos sin darnos cuenta.

- Dumpster Diving: se le conoce como el proceso de buscar en nuestra basura para obtener información útil sobre nuestra persona o empresa que luego puede utilizarse contra nosotros para otro tipo de ataques.

- Malware: el término se refiere de forma genérica a cualquier Software malicioso que tiene por objetivo infiltrarse en un sistema para dañarlo. Comúnmente se asocian como tipos de Malware a los virus, gusanos y troyanos.

- Virus: es un código que infecta los archivos del sistema mediante un programa maligno, pero para ello necesita que el usuario lo ejecute directamente. Una vez activo, se disemina por todo el sistema a donde el equipo o cuenta de usuario tenga acceso, desde dispositivos de Hardware hasta unidades virtuales o ubicaciones remotas en una red.

- Gusanos: es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por la red. A diferencia del virus, no necesita la intervención del usuario, ya que pueden transmitirse utilizando las redes o el correo electrónico. Son difíciles de detectar, pues su objetivo es difundirse e infectar a otros equipos, y no afectan inicialmente el funcionamiento normal del sistema. Su uso principal es el de la creación de redes zombies (Botnets), utilizadas para ejecutar acciones de forma remota como ataque de denegación de servicio (DoS) a otro sistema.

- Troyanos: similares a los virus, sin embargo, mientras que este último es destructivo por sí mismo, el troyano lo que busca es abrir una puerta trasera (Backdoor) para favorecer la entrada de otros programas maliciosos. Su misión es precisamente pasar desapercibido e ingresar a los sistemas sin que sea detectado como una amenaza potencial. No se propagan a sí mismos y suelen estar integrados en archivos ejecutables aparentemente inofensivos.

- Spyware: es un programa espía, cuyo objetivo es recopilar información de un equipo y transmitirla a una entidad externa sin el consentimiento del propietario. Su trabajo suele ser silencioso, sin dar muestras de su funcionamiento, llegando incluso a instalar otros programas sin que se perciban. Las consecuencias de su infección incluyen, además, pérdida considerable del rendimiento del sistema y dificultad para conectarse a internet.

- AdWare: su función principal es la de mostrar publicidad. Aunque su intención no es la de dañar equipos, es considerado por algunos una clase de Spyware, ya que puede llegar a recopilar y transmitir datos para estudiar el comportamiento de los usuarios y orientar mejor el tipo de publicidad.

- Ransomware[56]: este es uno de los más sofisticados y modernos ataques, ya que lo que hace es secuestrar datos (encriptándolos) y pedir un

[56]El Ransomware se ha convertido en la principal amenaza para la ciberseguridad mundial. Desde que el troyano WannaCry afectó en la primavera de 2017 al menos a 200.000 equipos y servidores de 150 países, poniendo 'contra las cuerdas' a importantes empresas, el uso de este tipo de ataques informáticos no ha dejado de aumentar y son cada vez más numerosos, sofisticados, peligrosos y masivos.

Si en sus inicios los atacantes se conformaban infectando ordenadores de consumo a cambio de unos pocos dólares, todos los informes apuntan que los ciberdelincuentes están enfocando su ámbito de actuación preferente al segmento empresarial, organizaciones, administraciones e infraestructuras públicas con Malware tan peligroso como 'CryptoWall', 'Babuk', 'Black Kingdom', 'Ryuk' o 'CryptoLocker' que destacan por su alto nivel de código y su capacidad de control de ordenadores y redes mediante el cifrado de archivos.

El número de víctimas por Ransomware es ya interminable. La última conocida (abril 2021) ha sido la cadena de tiendas Phone House, pero la lista de los últimos meses es amplísima: la multinacional Acer; el estudio CD Projekt Red; la asociación deportiva NBA; el líder en cámaras Canon; el desarrollador japonés Capcom; la firma de seguros Mapfre; municipios y hospitales estadounidenses o la infraestructura del SEPE, el Servicio Público de Empleo Estatal de España que gestiona subsidios y maneja datos personales de millones de desempleados.

Solo es un ejemplo de afectados y, además, se sospecha que otras empresas han recibido ataques, aunque han preferido no divulgarlos públicamente ante la pérdida reputacional que suponen estos incidentes que son una lacra que parece imparable. Realmente, no hay sistema operativo, plataforma, dispositivo o red informática que esté a salvo, porque el Ransomware emplea cualquier tipo de vulnerabilidad, tipo de Malware o de ataque para secuestrar los equipos. Y no en todas las ocasiones es detectado a tiempo por los sistemas de seguridad y Software antimalware.

Teniendo en cuenta que un Ransomware típico puede infectar dispositivo móviles, ordenadores personales, servidores o redes, bloqueando su funcionamiento y/o acceso a una

rescate por ellos. Normalmente, se solicita una transferencia en dinero electrónico (Bitcoins), para evitar el rastreo y localización. Este tipo de ciberataque va en aumento y es uno de los más temidos en la actualidad.

- Stalkerware: se trata de un programa que permite el seguimiento y monitorización de la actividad del usuario en un dispositivo móvil como teléfono, tableta o computadora. El problema de este tipo de programas es que no han sido creados puntualmente para el espionaje y el acoso, sino para el intercambio de datos entre dispositivos de manera más sencilla. Y qué sí se instalan sin el consentimiento de la persona, permite espiar sus comunicaciones y toda su actividad gracias a las funcionalidades y sensores incorporados en el dispositivo.

- Escaneo de Puertos: técnica empleada para auditar dispositivos y redes con el fin de conocer qué puertos están abiertos o cerrados, los servicios que son ofrecidos, así como comprobar la existencia de algún cortafuegos (Firewall), la arquitectura de la red, o el sistema operativo, entre otros aspectos. Su empleo permite al atacante realizar un análisis preliminar del sistema y sus vulnerabilidades, con miras a algún otro tipo de ataque, pues cada puerto abierto en un dispositivo, es una potencial puerta de entrada al mismo.

- Phishing: no es un Software, se trata más bien de diversas técnicas de suplantación de identidad para obtener datos privados de las víctimas, como contraseñas o datos bancarios. Los medios más utilizados son el correo electrónico, mensajería o llamadas telefónicas, y se hacen pasar por alguna entidad u organización conocida, solicitando datos confidenciales, para posteriormente ser utilizado por terceros en su beneficio.

- Quishing: es una técnica de Phishing que utiliza códigos QR[57] para engañar a las personas y redirigirlas a sitios Web fraudulentos, escribir un

parte o a todo el equipo apoderándose de los archivos con un cifrado fuerte y exigiendo una cantidad de dinero como "rescate" para liberarlos, el mejor (y casi único) de los consejos en ciberseguridad es la prevención con las copias de seguridad como máximo exponente. La opción de pagar el rescate para recuperar el acceso a los archivos es muy negativa para la industria ya que retroalimenta aún más esta amenaza.

[57] Un código QR, nomenclatura para Quick Response o Respuesta Rápida, es una imagen escaneable de una matriz de dos dimensiones que pertenece a la familia de los códigos de barras que podríamos encontrar en otros productos, diseñado inicialmente en 1994 para la industria automotriz en Japón. Estos códigos son capaces de almacenar información hasta un total de 7089 caracteres numéricos o 4296 caracteres alfanuméricos en la versión

correo electrónico o un mensaje SMS, añadir un contacto a tu agenda, añadir un evento a tu calendario, añadir credenciales de acceso a una red WiFi, realizar un pago Online, iniciar una llamada telefónica, enviar información sobre tu localización a una app, empezar a seguir a alguien en redes sociales o te puede llevar a descargar un Malware.

- Whaling: es un método para simular ocupar cargos de nivel superior en una organización con el objeto de conseguir información confidencial u obtener acceso a sistemas informáticos con fines delictivos.

- El Smishing: ocurre cuando se recibe un mensaje de texto corto (SMS) en el teléfono celular, por medio del cual se solicita al usuario llamar a un número de teléfono o ir a un sitio Web.

- El Vishing: es la estafa que se produce mediante una llamada telefónica que busca engañar, suplantando la identidad de una persona o entidad para solicitar información privada o realizar alguna acción en contra de la víctima.

- Juice-jacking o Video-jacking: son los nombres que se han puesto a los procesos por los cuales, a través de un puerto (generalmente USB) nos conectamos a un puerto Hackeado, de esta forma el ciberdelincuente puede instalar, grabar datos, tomar video o sacar datos de nuestros dispositivos móviles. Esto se ha vuelto común en los puertos de recarga de energía públicos a través del puerto USB. Si se hará uso de este tipo de servicios, es recomendable adquirir un dispositivo del tipo PortaPow de carga rápida con adaptador USB que inhabilitan los pines de datos permitiendo sólo la carga del dispositivo.

- Keylogger (registrador de teclas): es un Software malicioso o dispositivo en Hardware -generalmente conectado al teclado- que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente usarlas para robar información privada.

- Criptomining es un Malware diseñado para la extracción de Criptomonedas en nuestros dispositivos. Si el usuario accesa a un sitio Web que esté infectado, el Malware se puede descargar de forma inadvertida a través de una descarga automática y nuestro dispositivo comenzará a

40 de estos códigos.

desenterrar una moneda criptográfica seleccionada para los Hackers; la infección será notoria por un uso intensivo de nuestro dispositivo.

- Botnets (Redes de robots): Son computadoras o dispositivos conectados a la red (teléfonos inteligentes, tabletas, etc.) infectados y controlados remotamente, que se comportan como robots (Bots) o zombies, quedando incorporados a redes distribuidas, las cuales envían de forma masiva mensajes de correo Spam o código malicioso, con el objetivo de atacar otros sistemas o dejarlos fuera de servicio.

- Denegación de Servicios: tiene como objetivo inhabilitar el uso de un sistema o computadora, con el fin de bloquear el servicio para el que está destinado. Los servidores Web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, comienzan a ralentizarse o incluso bloquearse y desconectarse de la red. Existen dos técnicas para este ataque: la denegación de servicio o DoS (Denial of Service) y la denegación de servicio distribuido o DDoS (Distributed Denial of Service); la diferencia entre ambos es el número de equipos de cómputo que realizan el ataque. En el primero, las peticiones masivas al servicio se realizan desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que no tiene capacidad de respuesta y comienza a rechazar peticiones (denegar el servicio); en el segundo, las peticiones o conexiones se realizan empleando un gran número de computadoras o direcciones IP, todas al mismo tiempo y hacia el mismo servicio objeto del ataque, de forma general, las computadoras que lo realizan se encuentran infestadas, formando parte de una Botnet, y comportándose como zombis.

- Ataque MITM (Man In The Middle): conocido como "hombre en el medio", ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa simulando una falsa identidad. En este sentido, el atacante tiene control total de la información que se intercambia, pudiendo manipularla a voluntad, sin que el emisor y el receptor lo perciban rápidamente. Es común que se realice empleando redes WI-FI públicas y abiertas, y es muy peligroso ya que se puede obtener información sensible de las víctimas, y es difícil identificarlo si no se poseen los mínimos conocimientos sobre el tema.

- Rootkit: es un tipo de Malware diseñado para infectar una PC, el cual permite instalar diferentes herramientas que dan acceso remoto al equipo de cómputo. Este Malware se oculta en la máquina, dentro del sistema operativo y sortea obstáculos como aplicaciones antimalware o algunos productos de seguridad. El Rootkit contiene diferentes herramientas maliciosas como un módulo para robar los números de tarjeta o cuentas bancarias, un Bot para ataques y otras funciones que pueden desactivar el Software de seguridad.

- SIM Swapping: es la duplicación del SIM de un número telefónico que permite a un atacante usurpe nuestra identidad, pudiendo autentificarse por medio de SMS en diversos servicios que usen la autentificación de dos pasos, incluyendo los servicios bancarios.

- SIM Jacker: es el envió de un mensaje malicioso al dispositivo destino, que si se abre el enlace adjunto, el dispositivo inteligente queda comprometido y se puede extraer toda la información del mismo incluyendo la ubicación.

- 0-Day (día cero): es una nueva vulnerabilidad para la cual no se han creado parches o revisiones, y que se emplea para llevar a cabo un ataque. El nombre se debe a que no existe ninguna revisión para mitigar el aprovechamiento de la(s) vulnerabilidad(es), estas pueden ser utilizadas para qué troyanos, Rootkits, virus, gusanos y otros Malwares se propaguen e infecten más equipos.

- IP Spoofing: el ciberdelincuente consigue falsear su dirección IP y hacerla pasar por una dirección válida en la cual confiamos, de este modo, consigue saltarse las restricciones y puede hacernos conectar a una Web maliciosa.

- Web Spoofing: consiste en la suplantación de una página Web real por otra falsa. La Web falsa es una copia del diseño original, llegando incluso a utilizar una URL muy similar para que demos nuestras credenciales de acceso.

- Email Spoofing: consiste en suplantar la dirección de correo de una persona o entidad de confianza para solicitarnos datos o que descarguemos archivos maliciosos.

- DNS Spoofing: a través de programas maliciosos específicos y aprovechándose de las vulnerabilidades en las medidas de protección, los atacantes consiguen infectar y acceder a nuestro Router suplantando la DNS (Domain Name System). Así cuando tratamos de acceder a una determinada Web desde el navegador, este nos lleva a otra Web elegida por el atacante.

- Sniffing: se trata de una técnica utilizada para escuchar todo lo que se transmite dentro de una red, de esta forma se monitorea el tráfico y se puede capturar información que viaja de forma no cifrada para analizarla y hacerse de nuestros datos.

- Ataque de inyección de SQL (Structured Query Language): es aprovechar una o más vulnerabilidades de servidores SQL que hace que se divulgue información confidencial de la base de datos que de otra manera no haría al inyectar código SQL malicioso. Esto representa un riesgo enorme si la base de datos almacena información de identificación personal, como números de tarjetas de crédito, información personal y contraseñas.

- Baiting o Gancho: se sirve de algún medio físico como una unidad USB infectada que el atacante deja al alcance de los usuarios, para que cuando este lo introduzca en su equipo se infecte. También puede usar anuncios en Webs con la que promociona cursos o premios que nos inciten a compartir datos o descargar Software malicioso.

- USB Killer: un dispositivo de este tipo, es similar a una Unidad Flash USB que envía sobretensiones de alto voltaje al dispositivo al que está conectado, lo que puede dañar los componentes del Hardware. El dispositivo extrae corriente eléctrica del conector eléctrico USB del equipo al que esté conectado, pasándola a sus condensadores, hasta que alcanza un alto voltaje y entonces libera el alto voltaje en los pines de datos. Las versiones 2, 3 y 4 del dispositivo pueden generar un voltaje de 110 a 220 voltios, súcientes para dañar irremediablemente el dispositivo al que se inserte.

En general, para poder llevar a cabo alguno de estos ataques, los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas, deben contar con una determinada motivación o finalidad, y se

tiene que dar además una oportunidad que facilite el desarrollo del ataque, como podría ser un fallo en la seguridad del sistema informático elegido.

3.5 Dicen que si no Pagas por un Producto, Entonces el Producto Eres Tú.

¿Cuál es el modelo de negocio de empresas tecnológicas como Facebook? usar Google, Facebook, Messenger, Instagram y WhatsApp es completamente gratis. Y pese a ello, por ejemplo Facebook saca cada vez más dinero por usuario. Esto es posible gracias al uso que Facebook hace de nuestros datos. Teóricamente, y escándalos por fallos de seguridad al margen, Facebook no vende nuestros datos a terceros, sino que vende a terceros el acceso a nosotros gracias al uso de nuestros datos.

Así, las empresas tecnológicas (no importa si pagamos o no por un servicio o producto) van detectando nuestros gustos e intereses en base al dispositivo desde el que accedemos, las páginas que seguimos, nuestro historial de navegación y otros factores, y crea un perfil sobre cada uno de nosotros. Luego vende espacios de nuestro Feed a las empresas que busquen gente como nosotros (franja de edad determinada, localización, aficiones...). Y ya se está planteando formas de ir más allá mediante acuerdos con terceros, como uno con la banca para poder saber el dinero que tenemos en nuestra cuenta.

Esta red publicitaria que tan optimizada está merece el aplauso por su logro técnico, pero quizás no sea tan plausible si tenemos en cuenta ese rastreo tan agresivo y la escasa preocupación de las empresas por la privacidad de sus usuarios.

Por otro lado, el uso generalizado de las redes sociales entraña algunos riesgos que, siguiendo recomendaciones básicas, se pueden evitar. Como cualquier comunidad frecuentada por miles de usuarios (o, como sucede a veces con las redes sociales, por miles de millones), se deben conocer los mecanismos de control y de seguridad para poder utilizarlos con fiabilidad para mantener nuestra privacidad y es por eso que el usuario tiene que ser especialmente cuidadoso con el uso que hace de la red social, a continuación daremos algunas recomendaciones:

- No necesitamos informar de todo y a todos, y menos con información sensible. Por ello, cuanta menos información pongamos, mejor.

- A menudo publicamos notas o mensajes en el muro de un amigo. Esto también es visible para otros usuarios de Facebook o de la red social que sea.
- Se dice que una foto vale más que mil palabras. Estamos dando información sobre nuestros hábitos, nuestros movimientos, a posibles atacantes.
- Hay que asegurarse de que nuestro contenido en las redes sociales sea visible solo para amigos y familiares.
- Google, Twitter, Facebook e Instagram usan el geoetiquetado mediante el GPS para ayudar a los usuarios a marcar la ubicación donde se hizo una foto, vídeo y ayudar a que el perfil sea más «social». Cualquier usuario puede interpretar fácilmente información como nuestro estado económico, estilo de vida, lugares frecuentes y la rutina diaria a través de los medios con etiquetas geográficas.
- En una red social lo normal es que cada usuario se identifique con su nombre y apellido real y que aporte datos personales, como si estudia o trabaja, con quién se relaciona o en qué ciudad vive.Esto hace que su exposición pública sea mucho mayor que antes, esto implica la pérdida del anonimato algo que antes era común y habitual en internet.
- En las redes sociales, una vez que se pulsa el botón de "publicar", esa información es enviada a los contactos del usuario. Eso significa que si más adelante el usuario se arrepiente de lo dicho, publicado o mostrado y trata de borrarlo, solo conseguirá eliminarlo de su propio perfil pero no de internet.
- Quizás lo más importante de estos consejos para mantener la seguridad en redes sociales es el sentido común en lo que publicamos y comentamos en ellas.

Acuerdos de Privacidad la lectura de los acuerdos de privacidad[58] orientará al usuario sobre qué datos se comparten o no, y también se ofrece

[58] Si de verdad leyéramos los términos y condiciones de uso de plataformas Online seleccionadas (datos de abril 2020), tardaríamos (con una velocidad de 240 palabras por minuto) aproximadamente:

la opción de seleccionar o anular las opciones de privacidad, seguridad o administrativas escogidas para proteger la cuenta y el dispositivo.

Al registrarte en una cuenta de redes sociales, por defecto, toda la información anotada en un perfil se hace pública, lo que significa que cualquier persona puede acceder al contenido que hayas registrado en una cuenta. Sin embargo, las necesidades y preferencias de privacidad varían de persona a persona. Mientras que algunos usuarios prefieren tener una mayor exposición y así poder promocionar su contenido en redes sociales, otros prefieren incluir muy poca o ninguna información.

Para lograr una mayor protección del usuario y su información, es importante evaluar en qué medida la persona está dispuesta a incluir información personal en su perfil. Por consiguiente, ten en cuenta lo siguiente al:

- Seleccionar un nombre de usuario: el nombre de usuario es el "nombre digital" que una persona se asigna a sí misma o a su organización para ser identificada en línea. Si existe la preferencia de no ser fácilmente identificada en ninguna plataforma, pero poder continuar usando estas redes, la persona puede asignar y usar un seudónimo que puede estar relacionado o no con esa persona. Además, la persona puede cambiar su nombre de usuario en cualquier momento simplemente ingresando a la configuración de su (s) cuenta (s). El nombre de usuario no tiene que ser coherente en todas las redes sociales; estas pueden variar según las preferencias en cada una.

- Incluir una imagen en la cuenta: el usuario tiene la opción de personalizar una cuenta con la inclusión de una foto del perfil. Cuando un usuario prefiere no ser identificado, se sugiere elegir una imagen en la que no pueda ser identificado y cambiarla cuando sea necesario. Ten en cuenta que cuando se usa la misma imagen en todas las redes sociales, la simple búsqueda de imágenes puede llevar a otras cuentas.

- Incluir una ubicación: cuando se activan los servicios de ubicación en la plataforma de redes sociales, estos permiten a los usuarios rastrear el

Microsoft 1:03:30 s (15,260 palabras), Spotify 35:48 s (8,600 palabras), Tik Tok 31:24 s (7,459 palabras), Apple 30:30 s (7,314 palabras), Zoom 30:12 s (7,243 palabras), Tinder 25:54 s (6,215 palabras), Uber 25:36 s (5,658 palabras), Twitter 25:30 s (5,633 palabras), LinkedIn 18:06 s (4,346 palabras), Facebook 17:12 s (4,132 palabras), Amazon 14:12 s (3,416 palabras), YouTube 13:42 s (3,308 palabras, Netflix 11:00 s (2,628 palabras), Instagram 9:42 s (2,451 palabras).

origen de cualquier actividad de medios en línea. Es importante tener en cuenta que una vez que se activa esta función, permanecerá activa hasta que se elija deshabilitarla en la configuración de privacidad. A pesar de que se permitía que esta característica estuviera activa en el pasado, las plataformas tienen la funcionalidad de deshabilitar la ubicación de cualquier contenido que se haya publicado en sus cuentas.

Sin embargo, aunque un usuario active o desactive la función de compartir la ubicación, potencialmente, la ubicación de un usuario podrá ser descubierta por el contenido que comparta o las imágenes que haya elegido para compartir.

3.6 Datos que Recopila Google

Desde el escándalo de Cambridge Analytica[59] en 2018, poco a poco todos nos hemos ido haciendo más conscientes de nuestra privacidad, y cómo las grandes empresas recopilan nuestros datos casi sin que nos demos cuenta. Ya no solo Facebook y las redes sociales, ya que hay otras empresas como Google que pueden recopilar muchos más datos sobre lo que hacemos cada día.

En parte, esto se debe a que es una empresa que ofrece una gran cantidad de servicios gratuitos que utilizamos casi sin pensar, y en otra, porque es la dueña de todo lo que buscamos en la red (si usamos sus productos y servicios). Para hacerme una mejor idea de hasta dónde llega, podemos descargar todos nuestros datos y sí los revisamos es seguro que tendremos una desagradable sorpresa, que nos llevan a la conclusión de que Google sabe mucho más sobre nosotros que la propia Facebook, como por ejemplo, por dónde he viajado y qué aplicaciones utilizo y cuándo.

Algunos de estos datos los puedes encontrar fácilmente en algunas páginas de datos. Pero para otros, hemos utilizado la herramienta Google Takeout para descargar una copia de seguridad de todo lo que tienen sobre nosotros. Ya es bastante significativo que esta copia ocupe varios Gigas. Algo que debes saber es que puedes configurarlo para que muchos de los datos que Google tiene sobre ti se autodestruyan cuando haya pasado determinado tiempo.

Una cosa que hay que tener en cuenta es que Google no tiene por qué estar vendiendo o revisando minuciosamente estos datos, aunque tampoco

[59] Se le acusa de tratar de influenciar los resultados de las elecciones presidenciales de 2016 en los Estados Unidos de Norteamérica.

hay manera de asegurarse de que no lo hagan con alguno. Sin embargo, en algunos casos nos parece excesivo incluso el simple hecho de que recopilen algunos de ellos. Para que sepas de lo que estamos hablando, aquí tienes una lista del tipo de datos personales que he visto que Google recopila.

Lo primero que llama la atención al mirar los datos de Google, es que sabe por dónde te has estado moviendo. Por ejemplo, tiene una función de cronología en la que puedes ver todos los movimientos que ha ido registrando sobre ti cuando tienes habilitado el historial de ubicaciones de Google Maps. Este suele estar activado por defecto en tus dispositivos, lo que quiere decir que si no cambias la configuración deliberadamente seguirá todos tus pasos a través de tu móvil, tableta o cualquier otro dispositivo con el que estés identificado con tu cuenta de Google.

Todos estos datos Google te los va presentando de forma ordenada y cronológica, mostrándote a qué hora has salido de un sitio, el medio de transporte por el que has ido y qué paradas has hecho. Sorprende la minuciosidad con la que Google lo registra todo. Además, en el caso de que te hayas ido de viaje sacando muchas fotos, Google también va a saber dónde y cuándo sacaste las fotografías con tu móvil, y todo te lo va a mostrar de forma ordenada viendo cómo hiciste el camino y dónde hiciste las fotos. Incluso distingue los trayectos que hiciste en coche y los que has hecho a pie. Esto lo hace utilizando los metadatos de tus fotos y cruzándolos con la información de ubicaciones que recopila.

Y más allá de esta herramienta, en la copia de seguridad de Google también puedes encontrar otras sorpresas. Por una parte, hay una carpeta con un historial de ubicaciones, en la que puedes ver las coordenadas por las que te has movido en los últimos días y la manera en la que lo has hecho. Es como lo de Google Maps, pero con el código en bruto.

También guarda las actividades que hayas registrado utilizando Google Fit. Aquí puedes encontrar dos carpetas diferentes, una con todos los ejercicios que has hecho utilizando esta aplicación, con horas y coordenadas, y otra con un archivo diario en el que se puede ver todos los movimientos agregados en cada momento. Da igual que lleves años sin utilizar la aplicación guarda los datos obtenidos de aplicaciones de terceros al vincularlas con el servicio.

Google también tiene una sección Mi Actividad en la que recoge y almacena todas las búsquedas que haces en Internet, así como el contenido que consumes dentro de portales pertenecientes a Google. Aquí no solo vas a encontrar las búsquedas hechas a través del buscador, sino las búsquedas realizadas en Chrome y tu Android.

La verdad es que al mirar mi cronología no he podido evitar sentirme un poco incómodo, sobre todo porque todos los datos están perfectamente organizados y van acompañados de enlaces. De esta manera, puedes saber que has buscado determinados términos y volver a pulsar sobre ellos para ver los resultados de búsqueda, pero también puedes saber qué perfiles de Twitter o Facebook has visitado o las páginas a las que has entrado.

Además de esto, Google también recopila cuando utilizas otras plataformas como Stadia. Incluso si simplemente pulsas en el botón de Discover de la aplicación de Google para ver los temas que la propia Google considera importantes para ti, va recopilando cuáles son los temas sobre los que te ha mostrado información cada vez.

Es más, dentro de algunas páginas también te dice en qué secciones has navegado. Esto se vuelve un poco más preocupante con el tema de los foros, ya que te dice el título de cada hilo que has visitado dentro de un mismo foro, e incluso te ofrece enlaces para volver a él.

La Web también registra cuántas veces utilizas cada aplicación móvil y lo que es peor, todos estos datos siguen apareciendo aunque borres el historial de Chrome. He probado borrar las páginas a las que he entrado hoy con el navegador, y estas seguían apareciendo en la página de My Activity.

¿Y qué implicaciones tiene esto? Pues no sólo que Google sabe exactamente todo lo que haces en Internet si utilizas sus productos, sino que cualquiera que se ponga frente a tu computadora, tableta o teléfono inteligente (si tiene acceso a tu cuenta) va a poder saberlo, ya que al entrar a My Activity Google no pide que confirme mi identidad. Así que cualquiera puede con relativa facilidad tener acceso a esta información.

En resumen Google tiene acceso a:

- Tu nombre, tu dirección, tu edad, tu correo electrónico. Tu modelo de teléfono, tu proveedor de telefonía celular, tu plan y tu consumo telefónico y de internet.

- Las palabras que usas con más frecuencia dentro de tus correos electrónicos. Todos los correos que hayas escrito o recibido, incluido Spam. Los nombres de tus contactos y sus direcciones y teléfonos.

- Las fotografías que tomas con tu teléfono Android, aunque las hayas borrado y aunque no las subas nunca a ninguna red social. Los sitios a los que vas, dentro y fuera del país; la fecha en la que fuiste y la ruta

que tomaste. Qué tan rápido llegaste. La tarjeta de crédito o débito que usas para pagar.

- Todos los sitios de internet que has visitado en Google, con qué frecuencia y lo que viste dentro de cada uno. En qué idioma buscas. A qué hora navegas. Con quién has hablado vía Hangouts. Qué videos te gustan. Qué música oyes, etc.

Para tratar de minimizar nuestra huella digital, si soy usuario de los servicios de Google puedo desactivar todos los servicios de rastreo a los que me da opción en su página de "Administrar tu cuenta de Google", no es notoria la degradación del servicio por dichas desactivaciones. Pero esto no impide que Google y servicios de terceros recolecten y transmitan nuestros datos, solo no se almacenarán en nuestra cuenta, ni tendremos acceso a los mismos.

También puedo prescindir de los servicios de Google usando otras alternativas no tan invasivas como describimos más adelante en este texto.

3.7 ¿Cómo me Protejo?

Algunas normas básicas de ciberseguridad para nuestra seguridad, tener privacidad y evitar la vigilancia son:

- Usar contraseñas largas, robustas (incorporar mayúsculas, minúsculas, números y símbolos) y diferentes para cada servicio que lo solicite, para facilitar el manejo de las contraseñas es recomendable el uso de gestores de contraseñas.

- Cifrar Dispositivos, Discos y Unidades de Respaldo para mantener la confidencialidad de nuestra información.

- Mantener actualizado el sistema operativo y las aplicaciones (sólo instalar las necesarias) de nuestros dispositivos además de usar mecanismos que coadyuven en la seguridad como cortafuegos, antivirus, entre otras aplicaciones de seguridad.

- Generar respaldos periódicos -compactados y cifrados- de nuestra información y garantizar que es posible restituir nuestros datos de dichos respaldos (una buena estrategia de respaldo es la siguiente: mantener tres copias de cualquier fichero importante -una principal y dos

respaldos-, mantener los ficheros en dos tipos distintos de almacenamiento para protegerlos ante distintos riesgos y almacenar una copia de seguridad fuera de nuestra casa u oficina).

- Para ciertas actividades en la red o el uso de programas poco confiables es recomendable el uso de máquinas virtuales que limitan los posibles daños por programas maliciosos.

- Al navegar en internet es necesario hacerlo de forma segura para no exponernos de forma innecesaria, mediante un uso seguro y aceptable de las herramientas en la Nube.

- Conocer las medidas mínimas de protección para una navegación segura en internet.

- Conocer las técnicas usadas en ataques de inteligencia social, para no ser víctimas de la ciberdelincuencia.

- Al hacer uso de videoconferencias conocer las políticas de privacidad y las medidas de seguridad para no exponernos a ciberacoso y pérdida de datos.

- Hacer un uso correcto de los dispositivos personales cuando estos son usados para el trabajo.

- Uso de escritorios remotos y virtuales como una forma de mitigar los riesgos cuando se trabaja de forma remota.

Entre otras tantas cosas que el usuario actual de las Tecnologías de la Información y la Comunicación (TIC) debe dominar. Además, debemos conocer algunas recomendaciones útiles para reducir nuestra huella en internet, como:

- No compartir nuestro correo electrónico y número telefónico, pese a que es habitual utilizarlos para registrarnos en sitios Web, si los compartimos libremente por internet nos exponemos a ser víctimas de Spam, Phishing y todo tipo de ciberataques basados en ingeniería social.

- El uso de cuentas de correo alternativas nos permite registrarnos en diferentes sitios Web sin utilizar datos y/o cuentas personales o de trabajo.

- Usar cuentas de correo seguro, anónimo y bidireccional como el servicio de Tutanota, Mailfence o ProtonMail. O usar el modo confidencial -en el cual podemos establecer fecha de vencimiento y contraseña para cada correo- al enviar correos desde cuentas Google.

- Acceder a las opciones del navegador para eliminar cada cierto tiempo la información almacenada en formas de Cookies, Caché o el historial de navegación.

- El uso de modo privado o incógnito[60] en el navegador nos permite no almacenar información sobre las páginas Web visitadas ni se guardan las Cookies, ya que se eliminarán al salir del navegador.

- Evitar revelar información sensible en redes sociales sobre nosotros, familia y conocidos, en medida de lo posible debemos vigilar lo que publicamos, quién puede verlo y configurar las opciones de privacidad.

- El uso de Webs seguras (https y certificados digitales) aseguran que la información que intercambiamos con ellas, como datos bancarios o contraseñas viajen de forma cifrada.

- Usar navegadores especializados (Tor) y lugares de búsqueda de información (DuckDuckGo) que nos permitan una navegación segura al no guardar lo que buscamos, ni los sitios donde accedemos.

- El uso del GPS en nuestros dispositivos móviles es una gran herramienta en nuestra vida digital, pero debemos tenerlo activado sólo cuando sea necesario, ya que muchas aplicaciones comparte nuestra ubicación en tiempo real sin nuestro conocimiento y alguien puede conocer donde vivimos, los lugares que frecuentamos o cuando no estamos en casa.

[60] En Chrome y otros navegadores Web, el modo incógnito -del cual Google sostiene que este modo- está diseñado para evitar el almacenamiento local de datos, y realmente no protege nuestra privacidad, aunque otros usuarios en el mismo dispositivo no verán la actividad en modo incógnito, los sitios Web y servicios, incluidos los de Google, aún pueden recopilar datos. La actividad, como descargas, favoritos y elementos de la lista de reproducción, se almacenará.

Cabe mencionar que ningún navegador ofrece el 100% de privacidad ni anonimato al usuario, lo que si, es que entre los diferentes navegadores existentes, podremos encontrar navegador web (como por ejemplo Brave) que ofrecen capas adicionales de protección de los datos del usuario, pero esto no los vuelve 100% eficientes en ello, pues incluso navegadores como Tor (para la Dark Web) tiene sus fallos.

- Al tomar fotografías o vídeos desactivar el guardado de datos *Exif* (Exchangeable Image File) también conocidos como metadatos: datos sobre la cámara, datos sobre la fotografía y datos sobre el origen como ubicación por GPS, etc.
- Nunca tomar vídeos o fotos comprometedoras, de carácter íntimo o sexual y menos publicarlas, ya que suponen una gran amenaza a nuestra seguridad y pueden tener consecuencias muy graves, como la exposición pública, extorsión o el ciberacoso.
- No compartir fotos, vídeos o audios de menores.
- No debemos compartir vídeos, fotos o audios de terceros sin su aprobación, en especial los que contienen conversaciones privadas que difundan datos personales o información que podría considerarse como revelación de secretos y que la otra persona preferiría no difundir.
- Al emitir opiniones, quejas o comentarios subidos de tono u ofensivos en medios electrónicos nos expone a ser atacados o censurados y en ciertos casos podrían ameritar acciones legales.
- No publicar documentos personales en forma de fotos, vídeos o archivos (*.Docx*, *.PDF*, etc) ya que con su revelación nos expone a una suplantación de identidad y al uso de nuestros datos de forma fraudulenta.
- Cumplir las normas mínimas de protección de dispositivos personales en redes corporativas.
- Hacer uso correcto de escritorios remotos y virtuales en equipos personales para el trabajo remoto.

4 Recomendaciones de Ciberseguridad

Como usuarios de equipos de cómputo -incluidas las computadoras personales (PC), Laptops, los teléfonos inteligentes y las tabletas- tenemos poca o nula capacitación en cuanto a las normas básicas de ciberseguridad, las más importantes las discutiremos en esta sección.

4.1 Uso de Contraseñas Robustas

Las contraseñas protegen la información que contienen los dispositivos y cuentas de los usuarios. No obstante, ante la cantidad de claves y combinaciones que cotidianamente se deben utilizar, la mayoría de las personas opta por contraseñas fáciles de recordar por la comodidad que esto implica, o bien, por la falta de conocimiento de lo fácil que puede ser para un ciberdelincuente obtenerlas. Para asegurar la efectividad de las contraseñas[61] y evitar el robo de éstas, es recomendable poner en práctica las siguientes acciones:

- Al generar las contraseñas de los dispositivos y cuentas se deben utilizar claves largas -mínimo 15 caracteres[62]- y únicas para cada caso, evitando utilizar la misma contraseña para diferentes dispositivos o cuentas[63].
- Se deben evitar las combinaciones sencillas como fechas de nacimiento, secuencias consecutivas, repeticiones de un mismo dígito o palabras simples como "password" o "contraseña".
- La mayor longitud de la contraseña, así como la incorporación de

[61] Para conocer la seguridad de una clave, podemos revisarla en:
https://howsecureismypassword.net/

[62] Solo para tener una idea del tiempo necesario para encontrar la clave de 13 caracteres aleatorios de símbolos, números, letras mayúsculas y minúsculas usando fuerza bruta en un solo core en el que se ejecuten más de mil millones de intentos por segundo se tardaría 9.6 millones años. Si se aumentan el número de cores los tiempos se acortaran de forma drástica, por ejemplo si se usa una supercomputadora que intente 100 millones de contraseñas por segundo bajaría de 9.6 millones a 96 años.
https://i.imgur.com/e3mGIFY.png

[63] Según una encuesta de Google y Harris Poll, el 52% de las personas reutiliza las mismas contraseñas para varias cuentas, y el 13% utiliza la misma para acceder a todo. Asegúrese de no formar parte de esas estadísticas. En su lugar, implante aplicaciones de gestión de contraseñas que obliguen a todo el mundo a utilizar un código único y aleatorio para cada cuenta y dispositivo.

mayúsculas, minúsculas, números y símbolos (#$,.-_%&*!?), contribuyen a que ésta sea más segura y difícil de vulnerar[64].

- Se debe evitar escribir contraseñas en papeles o tener archivos con esa información que sean fácilmente accesibles para otros.
- Habilitar el doble factor de autenticación o verificación en dos pasos. Esta medida es una capa adicional de seguridad disponible para cada vez más servicios en la que, además de la contraseña, durante el inicio de sesión se solicita información sobre otro medio al que sólo el usuario autorizado tiene acceso (por ejemplo, verificación para entrar al correo electrónico mediante la recepción de un código vía SMS, llamada o mensaje de WhatsApp).
- Es importante no facilitar a nadie, aunque así lo solicite, por ningún medio, contraseñas y/o códigos para el inicio de sesión.
- Es recomendable cambiar con frecuencia las contraseñas a efecto de evitar accesos no autorizados.
- Es recomendable usar un gestor de contraseñas[65] (como KeePassXC, KeePass, Bitwarden, Dashlane, NordPass, LastPass, Enpass, Keeper

[64] GnuPG y OpenSSl son herramientas en línea de comandos de seguridad en comunicaciones electrónicas en donde se utiliza criptografía de clave pública para que los usuarios puedan comunicarse de un modo seguro.

Para instalar el paquete GnuPG, usamos:

```
# apt install gnupg
```

para generar clave aleatoria de por ejemplo 32 caracteres, usamos:

```
$ gpg –gen-random –armor 1 32
```

Para instalar el paquete OpenSSL, usamos:

```
# apt install gnupg
```

para generar clave aleatoria de por ejemplo 32 caracteres, usamos:

```
$ openssl rand -base64 32
```

[65] Un administrador de contraseñas tiene dos funciones principales: (1) almacenar contraseñas, y (2) generar contraseñas seguras y únicas. Esta aplicación es esencialmente como un libro digital que almacena todas sus contraseñas usando una "clave maestra". Al ingresar esta clave, se le otorga acceso al resto de las contraseñas. Por lo tanto, dicha

Password Manager, Password Safe, Password Gorilla, UPM, Buttercup, Myki, Pass, 1Password, etc) para generar y almacenar las claves de acceso estrictamente necesarias y así evitar escribirlas en un papel. Este es un programa de seguridad que almacena de forma segura todas las contraseñas en una caja fuerte virtual cifrada, los hay locales a tu dispositivo o en línea.

- Aprovechar la autenticación multifactor (MFA). Entre las más comunes se encuentra la autenticación en dos factores (2FA o TFA), la cual requiere de dos formas distintas e independientes de identificación para acceder a una cuenta.

- Usar las redes wifi gratuitas con cautela y evitar abrir o compartir datos confidenciales. Desactive el bluetooth o la transferencia de archivos, ya que estas redes suelen ser objeto fácil de los ciberataques.

- Emplear un antivirus de alta calidad para proteger sus dispositivos. Este sistema debe ser capaz de detectar vulnerabilidades y amenazas en el equipo y de bloquear ataques antes de que sucedan.

Robo de contraseñas es uno de los problemas de seguridad informática más extendidos y alarmantes. Cuando ocurre, puede dejar daños financieros, tecnológicos o de otro tipo en personas y organizaciones de cualquier nivel. Proteger la información valiosa de los ataques de intrusos o Hackers es una acción que cada día cobra mayor relevancia. Por ese motivo, lo invitamos a seguir leyendo para conocer cómo resguardar sus contraseñas y cuáles son los métodos cada vez más sofisticados que usan los ciberdelincuentes para robarlas.

¿Qué es el robo de contraseñas? es un delito informático en el que se extraen datos que vulneran la privacidad y la seguridad de los usuarios. Para

clave o contraseña debe permanecer altamente protegida. Pero su segundo uso es mucho más práctico. El administrador de contraseñas genera automáticamente contraseñas que contienen una combinación compleja de mayúsculas y minúsculas, números, símbolos y caracteres especiales, que puede complicar el descifrado o la detección de la contraseña por parte de piratas informáticos. Al utilizar un administrador de contraseñas, se evita el error común de usar una sola contraseña en las diversas plataformas en línea, evitando así ataques de relleno de credenciales (credential stuffing).

ello, los Hackers roban o descifran las credenciales de acceso a un determinado sistema operativo o plataforma de información.

Luego, los usuarios maliciosos transfieren y almacenan de manera ilegal la información confidencial o financiera de una persona u organización, obteniendo réditos económicos de ello.

¿Cómo los Hackers roban contraseñas? estos son los métodos más utilizados por los Hackers para robar contraseñas y vulnerar los esquemas de Ciberseguridad:

1.- Ataques de fuerza bruta (brute-force attack) a través de este método, los piratas informáticos pueden descifrar las contraseñas débiles. Para hacerlo, utilizan herramientas que les permiten probar credenciales durante un gran número de intentos, hasta coincidir con los datos correctos. Para realizar este ataque, el ciberdelincuente toma en cuenta los requisitos de seguridad (como emplear mayúsculas, minúsculas y números), así como datos personales que los usuarios suelen introducir en sus contraseñas (fecha de nacimiento, por ejemplo).

2.- Phishing (suplantación de identidad) los cibercriminales emplean el Phishing y la ingeniería social para aprovecharse de las vulnerabilidades y brechas. Esto les permite aplicar mecanismos de manipulación psicológica para que las víctimas realicen acciones que aumentan el riesgo.

En estos ciberataques, los hackers emplean acciones como:

- Enviar a personas y organizaciones un correo electrónico con un asunto atractivo, en el cual insertan un archivo adjunto o enlace malicioso que, de hacer clic, descarga un Software malicioso (Malware) en el dispositivo de la víctima;
- Hacerse pasar por entidades conocidas y de confianza, como un banco, una organización pública o una empresa, a través de llamadas u otras formas de comunicación.
- Compartir páginas de destino (Landing Pages) que solicitan a las personas ingresar sus datos para iniciar sesión. Una vez el sitio Web registra los datos, este pasará a manos de los atacantes.

3.- Keylogger este método consiste en insertar un Malware en un ordenador o dispositivo móvil, permitiendo a los Hackers grabar información personal sin que el usuario pueda darse cuenta. Luego de ser instalado, este Software maligno registra las pulsaciones de teclas que hacen los usuarios. De esta manera, obtienen los nombres de inicio de sesión y contraseñas.

4. Claves genéricas este no es un método tan complejo para los Hackers. Consiste en probar contraseñas genéricas que suelen traer de fábrica los dispositivos. Por defecto, estas contraseñas no son tan difíciles, por lo que la recomendación para evitar este tipo de ataques es personalizar las credenciales una vez empieza a ser utilizado un determinado dispositivo.

5. Vulnerabilidades en las plataformas las propias plataformas muchas veces presentan vulnerabilidades en su seguridad. Los piratas informáticos buscan aprovecharse de ellas para robar nombres de usuarios y contraseñas. Un ejemplo de esto es cuando alguien realiza un registro en una red social y esta plataforma presenta algún problema. Sus datos quedan expuestos en la red, facilitando que un Hacker pueda apropiarse de ellos.

6.- Spyware (Software espía) esta es otra variedad de Software malicioso que puede ser utilizado para robar las contraseñas. Un spyware o software espía es capaz de grabar la pantalla de un dispositivo, recopilando así toda la información que el usuario va mostrando mientras interactúa con el sistema. Además, este software puede captar la información de discos duros y bases de datos para transmitirla a un ente externo.

7.- Diccionario de cuentas frecuentes los piratas informáticos poseen listas con las contraseñas más empleadas por los usuarios a lo largo de los años. Contraseñas como "password", "qwerty", "abc123", "123456" y otras similares son algunas de las más frecuentes. Estas listas usadas por los Hackers son conocidas como "diccionarios de ataque". Básicamente, prueban las contraseñas una por una hasta dar con la correcta. Para prevenir este tipo de ataques, se debe establecer contraseñas comunes y, por el contrario, utilizar otras más complejas.

8.- Ataque de diccionario este tipo de ciberataques es una variante más avanzada. Se basa en recopilar información de la víctima, como:

- Nombres de mascotas o de familiares;
- Fecha de nacimiento;
- Lugares en los que vivió anteriormente.

Para hacerlo, el atacante se vale de un Software que le permite probar todas las palabras de un diccionario basado en la información de la víctima y, en consecuencia, posibles contraseñas. De existir alguna coincidencia, el Hacker tendrá acceso a la cuenta. Estos ataques buscan aprovecharse de una mala práctica, muy frecuente, que es establecer contraseñas de una sola palabra para que sean fáciles de recordar, y que además se vinculan a un dato personal.

9.- Mirar por encima del hombro este es uno de los métodos menos sofisticados y, probablemente, el más antiguo, pero no deja de ser peligroso. Consiste en mirar por encima del hombro del usuario al pasar por delante de su smartphone o computadora, y a través de una mirada a la pantalla y el teclado, descifrar la contraseña. Este tipo de ataques puede ser más frecuente en sitios concurridos, como una biblioteca, cafetería o bar. Si suele ir a este tipo de locales es recomendable que tenga especial cuidado.

10.- Ataque de hombre en el medio (man-in-the-middle) en este ataque, el Hacker intercepta la comunicación entre dos o más personas, suplantando la identidad de uno u otro para tener acceso a la información y modificarla según desee. Luego de que el ciberdelincuente intercepta las comunicaciones, puede manipular las respuestas recibidas en uno de los extremos y hacerse pasar por el interlocutor legítimo. Con el uso de técnicas de ingeniería social puede enviar archivos adjuntos para instalar un software malicioso en el dispositivo de quien lo recibe.

4.2 Mantener Actualizado el Sistema Operativo y Aplicaciones

Mantener actualizados los sistemas operativos y las aplicaciones de los dispositivos, incluidas las computadoras personales (PC), los teléfonos inteligentes

y las tabletas[66]. Estas actualizaciones incluyen cambios importantes que mejoran el rendimiento y la seguridad de los equipos; muchos de estos programas, incluso, se actualizan de manera automática. Además de:

- Cifrar el disco (véase sección 4.3) donde reside el sistema operativo y nuestros datos, sin este cifrado cualquier persona con acceso físico a nuestro equipo de cómputo, tableta, teléfono o dispositivo electrónico puede copiar sus contenidos incluso si no tienen la clave de acceso a ellos.

- Instalar sólo aquellos programas y complementos que realmente uses, porque además de que pueden mermar la velocidad de tu equipo, es posible que estés cediendo más permisos de los que te imaginas.

- Activar funcionalidades de protección, como el cortafuegos (Firewall), incorporadas en los sistemas operativos más comunes. Un cortafuegos es la primera línea de defensa ante un ataque a tu red desde internet y permite proteger el equipo de programas maliciosos o atacantes que intenten conectarse al equipo de forma remota. Además, permite establecer reglas para indicar qué conexiones de red se deben aceptar y cuáles no. Al mismo tiempo, admite el normal intercambio de datos entre la computadora y servicios verificados de internet.

- En caso de usar el sistema operativo Windows o Android se debe instalar un antivirus[67], estos programas ayudan a proteger los dispositivos

[66] En el caso del sistema operativo Android hay una gran fragmentación de versiones en el mercado coexistiendo, esto debido a que los fabricantes y proveedores tienen un modelo de mercado que prioriza la venta de equipo nuevo y no la seguridad del usuario. Forzando a que las actualizaciones del sistema operativo dependan en gran medida del fabricante del dispositivo o del proveedor del servicio de telefonía, ya que ellos personalizan el sistema operativo, dificultando la actualización de los dispositivos. Lo que ocasiona que la gran mayoría de los dispositivos no reciban las actualizaciones de seguridad y nuevas versiones del sistema operativo publicadas por Android.

[67] Debido a que el Internet es una red abierta, cualquier computadora o dispositivo puede conectarse a este desde cualquier lugar. El uso de software antivirus sirve como un escáner inicial de cualquier actividad sospechosa o maliciosa a la que los usuarios están expuestos a través de las redes sociales. El software antivirus puede ayudar a supervisar la entrega de noticias y puede ofrecer un nivel adicional de protección en el evento que el usuario haga clic erróneamente en enlaces sospechosos que pueden contener Spam y diferentes tipos de virus, como gusanos . Pero tener instalado un software antivirus no es una protección general ya que no puede atrapar todo el malware; el dispositivo aún puede estar infectado.

contra la mayoría de los virus, gusanos, troyanos y otros tipos de Malware que pueden infectar a los dispositivos, por ello se recomienda:

- ◦ Instalar y mantener actualizados los antivirus, prefiriendo aquéllos que incorporan funcionalidades de protección contra Malware y cortafuegos (Firewall), también conocidos como "suites de seguridad".
- ◦ Evitar tener dos antivirus en un mismo dispositivo. Tener dos antivirus activos no significa mayor protección; de hecho, puede ocasionar diferentes problemas en el sistema. Un antivirus que esté trabajando se convertirá en un "Software malicioso" a los ojos del otro, el cual intentará bloquearlo y eliminarlo, y se corre el riesgo de afectar el desempeño del sistema por el consumo extra de recursos.
- ◦ Todas las instalaciones y actualizaciones de programas y aplicaciones deben hacerse desde el sitio Web oficial del fabricante o desde las tiendas oficiales de apps -verificando la identidad del autor de la aplicación-, evitando descargar e instalar aquéllas de dudosa procedencia.
- ◦ Deshabilitar la auto ejecución de memorias USB, para evitar que, por ese medio, se instalen programas maliciosos.
- ◦ En los sistemas operativos que lo soporten, habilitar la limpieza remota del dispositivo en caso de pérdida o robo.

- Nunca inserte ningún dispositivo de almacenamiento externo (USB[68], disco externo, unidad Flash, etc.) que no se hayan revisado exhaustivamente antes de ser usado.

Sin embargo, le agrega una capa de protección que puede ser beneficiosa para el usuario. Por eso es tan importante usar el sentido común también y desconfiar de cualquier mensaje que parezca extraño o sospechoso.

[68] Se debe tener cuidado con los llamados USB Killer, estos son dispositivos similar a una Unidad Flash USB que envía sobretensiones de alto voltaje al dispositivo al que está conectado, lo que puede dañar los componentes del Hardware. El dispositivo extrae corriente eléctrica del conector eléctrico USB del equipo al que esté conectado, pasándola a sus condensadores, hasta que alcanza un alto voltaje y entonces libera el alto voltaje en los pines de datos. Las versiones 2, 3 y 4 del dispositivo pueden generar un voltaje de 110 a 220 voltios, súcientes para dañar irremediablemente el dispositivo al que se inserte.

- Al desechar el dispositivo, es necesario reiniciarlo para borrar toda la información que pudiese contener.

4.3 Cifrar Dispositivos, Discos y Unidades de Respaldo

El cifrado de dispositivos, discos, unidades de respaldo -como los dispositivos USB-, datos o cifrado de archivos es un procedimiento mediante el cual los dispositivos, discos, archivos, o cualquier tipo de documento, se vuelven completamente ilegibles gracias a un algoritmo que desordena sus componentes. Así, cualquier persona que no disponga de las claves correctas no podrá acceder a la información que contiene. A menudo nos referimos a los datos cifrados como texto cifrado. El propósito del cifrado es proteger la confidencialidad de los datos digitales.

En el mundo criptográfico, cifrar es un procedimiento que utiliza un algoritmo matemático. Estos algoritmos modifican los datos, de manera que sólo sabiendo el mismo algoritmo se puede descifrar para saber qué es lo que se dice.

Como puede imaginarse, la protección de datos se ha convertido en una preocupación importante para las personas y compañías con el significativo crecimiento del volumen de datos y la sofisticación de la amenaza. A estos hechos, hay que añadir el riesgo que supone cada uno de nosotros lleva consigo grandes cantidades de datos confidenciales en sus ordenadores portátiles y dispositivos móviles.

¿Qué es cifrar? a pesar de los complicados cálculos matemáticos involucrados, la acción de cifrar datos no es difícil de entender. Simplemente, consiste en bloquear los datos mediante un código secreto que oculta su verdadero significado. De esta forma, si alguien accede a ellos, encontrará que la información carece de sentido. Y es que, para que los datos cifrados tengan sentido, se necesita la clave del código.

Existen dos tipos de cifrado: simétrico y asimétrico. En términos simples, el cifrado simétrico es la técnica más antigua y conocida. Utiliza una clave secreta para cifrar y descifrar los datos. Tanto el remitente como el receptor conocen la clave.

El cifrado asimétrico es un método más nuevo y también conocido como criptografía de clave pública. Utiliza dos claves en lugar de una: una pública y una privada. Las claves públicas permiten que cualquiera envíe información a otra persona, pero solo cada individuo conoce su clave privada.

Para qué sirve el cifrado de mensajes y otros datos sirve para hacer las comunicaciones más seguras, y lo mismo se puede decir a la hora de aplicarlo a internet. La primera funcionalidad para conseguirlo es la de la confidencialidad de los mensajes, ya que al no ir al descubierto, cuando tú le envías algo a otra persona, los algoritmos criptográficos de la aplicación ayudan a que no se pueda leer fácilmente si alguien lo intercepta en el camino.

Siendo la confidencialidad la primera de las ventajas que ofrece el cifrado de mensajes, la segunda podríamos decir que es la integridad. El encapsular un mensaje dentro de un sobre de cifrado, dicho así para hacerse una mejor imagen mental, ayuda que todo lo que haya cifrado se mantenga correcto y completo.

También hay algoritmos criptográficos que proporcionan mecanismos para verificar la identidad de la persona que envía un mensaje. Además, hay métodos de cifrado que también ayudan a vincular un documento o transacción a una persona o sistema de gestión concretas. Pero a nivel general, para lo que más se suele utilizar es para proteger las comunicaciones. Si tú envías un SMS se envía en texto plano, sin cifrar, y si un operador o alguna agencia interfiere el mensaje, puede leer todo lo que hay escrito. Sin embargo, aplicaciones como WhatsApp, Gmail o Telegram aplican cifrados para que esto no sea tan fácil.

¿Qué se debe cifrar? en términos generales, hay dos tipos de datos que se deben cifrar:

- Información de identificación personal. En este grupo se incluye cualquier tipo de información que otra persona pueda usar para identificar a un individuo de manera única. Esto incluye la licencia de conducir, número de seguridad social, etc. Los ladrones pueden usar esta información para robar una identidad, lo que les permite cometer delitos mayores, como solicitar tarjetas de crédito y préstamos a nombre de otra persona. Combatir esta clase de ataques requiere esfuerzos en muchos frentes. La información de identificación personal reside en los

teléfonos, tabletas y computadoras portátiles , por lo que esos dispositivos y su almacenamiento se deben cifrar.

- Información confidencial de Negocios y Propiedad Intelectual. Los datos a los que los empleados acceden cada día acerca de los clientes, los planes para un nuevo producto o los datos sobre la próxima campaña de marketing entrarían en este grupo. De toda esta información podrían sacar provecho los competidores y, por tanto, puede convertirse en objetivo de piratas informáticos.

Ante las dificultades para decidir si se deben o no cifrar algunos datos, basta con preguntarse si se destruirían antes de tirarlos a la basura, caso de estar en formato papel o si, en el caso de que se filtraran por accidente causarían daño a los empleados o clientes. En ambos casos, si la respuesta es afirmativa, hay que cifrar.

Cifrar Discos Los discos duros externos y los dispositivos USB son la manera perfecta de poder llevarnos en nuestros viajes todos nuestros archivos importantes. Pero cuando estos archivos son personales y privados es posible que no quieras que nadie pueda acceder a ellos en caso de que se te pierda el USB o te lo quiten de alguna manera.

Por eso, todos los sistemas operativos suelen darte la opción de aplicarles un cifrado y protegerlos con una contraseña de tu elección, un proceso diferente al de protegerlos contra escritura. Vamos a ver como hacerlo paso a paso con Windows con una de sus herramientas nativas, y también te diremos brevemente cómo hacer lo mismo en MacOS, Android y GNU/Linux pero de una forma aún más sencilla.

Cifrar en Windows la manera de cifrar unidades externas en Windows tiene un nombre: BitLocker. Se trata de una herramienta desarrollada por Microsoft que suele venir preinstalada en casi todas las versiones de su sistema operativo, pero que de no ser así puedes conseguir en su página de descarga, donde se pueden descargar sus versiones de 32 y 64 bits.

Cifrar en MacOS en el caso de que tengas un Mac el proceso es aún más fácil, ya que lo único que tienes que hacer es tener la unidad formateada, conectarla al equipo y dar Click derecho sobre su icono cuando aparezca en el

escritorio. En el menú desplegable sólo tendrás que elegir la opción: "Cifrar" para introducir con qué contraseñas lo quieres bloquear.

Cifrar en GNU/Linux en las distribuciones GNU/Linux por su parte también basta con dar Click derecho sobre la unidad, sólo que en este caso la opción a elegir es: "Formatear volumen". La clave aquí la tienes en el tipo de de formateo, ya que en él tendrás la opción Cifrado -LUKS o Cryptsetup-. De esta manera, formatearás el disco duro aplicándole directamente un cifrado con una contraseña que elijas.

Cifrar en Android siguiendo estos pasos podemos cifrar el disco:

1.- Ve a: "Ajustes".

2.- Selecciona: "Seguridad".

3.- Pulsa en: "Cifrar teléfono" y configura una contraseña (véase sección 4.1).

4.- Espera tranquilamente a que el proceso acabe, puede tardar más de media hora fácilmente.

Es importante destacar que la única forma de quitar el cifrado es reseteando de fábrica el dispositivo, lo que significa el borrado total del contenido que en él haya almacenado. Si tienes una tarjeta microSD insertada, los datos dentro también serán cifrados y no podrás acceder a ellos en otro dispositivo.

Cifrar Archivos

En Windows la herramienta que trae Windows preinstalada (ediciones Education, Pro y Enterprise) es un buen comienzo para cifrar nuestros datos.

Para ello, deberemos seguir los siguientes pasos:

1. Haz Clic con el botón derecho en un archivo o carpeta (o mantenlo presionado) y selecciona: "Propiedades".

2. Selecciona el botón: "Avanzados" y haz Clic en la casilla de verificación: "Cifrar contenido" para proteger datos.

3. Pulsa el botón: "Aceptar" para cerrar la ventana: "Atributos avanzados" y a continuación, selecciona el botón: "Aplicar" y después: "Aceptar".

Una vez cifrada la información, solo podremos acceder si disponemos de la clave de cifrado correcta.

En GNU/Linux y MacOS es posible cifrar archivos usando GnuPG, esta es una herramienta en línea de comandos de seguridad en comunicaciones electrónicas en donde se utiliza criptografía simétrica y de clave pública para que los usuarios puedan comunicarse de un modo seguro[69]. Dentro de las funciones de GnuPG se incluyen generar un par de claves, intercambiar y comprobar la autenticidad de claves, cifrar y descifrar documentos, etc. Para instalar el paquete GnuPG, usamos:

```
# apt install gnupg
```

Es posible cifrar archivos usando sólo una clave (véase sección 4.1) -cifrado simétrico- para cifrar el archivo. La clave que se usa para el cifrado simétrico deriva de la contraseña dada en el momento de cifrar el documento. El cifrado simétrico es útil para asegurar archivos cuando no sea necesario dar la contraseña a otros. Un archivo puede ser cifrado con una clave simétrica usando la opción *–symmetric*, por ejemplo:

```
$ gpg –symmetric doc
```

o

```
$ gpg -c doc
```

y podemos descifrar usando:

```
$ gpg doc.gpg
```

Para cifrar una carpeta, podemos usar:

```
$ tar -cvf archivo.tar directorio
$ gpg -c archivo.tar
```

o podemos usar el comando zip para compactar y cifrar, usando:

[69] Otras opciones son: ccrypt y mcrypt.

```
$ zip –encrypt archivo.zip archivo1 archivo2
$ zip -e archivo.zip archivo1 archivo2
$ zip -r –encrypt archivo.zip directorio
```

y podemos descifrar usando:

```
$ unzip archivo.zip
```

4.4 Generar Respaldos y Validar su Restauración

A veces, no importa cuán cuidadoso sea uno, existe la posibilidad de perder los datos o que te puedan Hackear[70]. Si ese es el caso, a menudo la única forma en la que puedes recuperar tu información (personal y de trabajo) es restaurar desde un respaldo. Es nuestro menester asegurarnos de realizar respaldos periódicos -preferentemente cifrados (véase sección 4.3) y comprimidos- de cualquier información importante y verificar que podamos restaurarla a partir de ellos. Es posible usar servicios en red como Google Drive y dispositivos USB para guardar en ellos los respaldos.

Debemos garantizar la disponibilidad, integridad y confidencialidad de nuestra información, tanto la que se encuentra en soporte digital, como la que se gestiona en papel. Una buena estrategia de respaldo es la siguiente:

- Mantener tres copias de cualquier fichero importante (una principal y dos respaldos).
- Mantener los ficheros en dos tipos distintos de almacenamiento para protegerlos ante distintos riesgos.
- Almacenar una copia de seguridad fuera de nuestra casa u oficina.

[70] El Ransomware se ha convertido en la principal amenaza para la ciberseguridad mundial. Desde que el troyano Wanna Cry afectó en la primavera de 2017 al menos a 200.000 equipos y servidores de 150 países, poniendo 'contra las cuerdas' a importantes empresas, el uso de este tipo de ataques informáticos no ha dejado de aumentar y son cada vez más numerosos, sofisticados, peligrosos y masivos.

Teniendo en cuenta que un Ransomware típico puede infectar dispositivo móviles, ordenadores personales, servidores o redes, bloqueando su funcionamiento y/o acceso a una parte o a todo el equipo apoderándose de los archivos con un cifrado fuerte y exigiendo una cantidad de dinero como "rescate" para liberarlos, el mejor (y casi único) de los consejos en ciberseguridad es la prevención con las copias de seguridad como máximo exponente.

Las copias de seguridad son nuestra salvaguarda básica para proteger la información. Dependiendo del tamaño y nuestras necesidades, los soportes digitales disponibles, la frecuencia y los procedimientos para realizar las copias de seguridad pueden ser distintos.

El soporte digital escogido dependerá del sistema de copia seleccionado, de la fiabilidad que sea necesaria y de la inversión que deseemos realizar. En la implantación de un sistema de copias debemos tener en cuenta al menos las siguientes consideraciones:

- Analizar la información de la que se va a realizar la copia, así como los sistemas y repositorios donde se encuentra. Debemos tener en cuenta las configuraciones de dispositivos en red, los equipos que dispongamos. Este paso debe permitirnos descartar información que no es necesaria respaldar o ficheros históricos de los que ya existen copias.

- Debemos definir el número de versión que vamos a almacenar de cada elemento guardado, y su periodo de conservación (es lo que se conoce como política de copias de seguridad).

La principal diferencia entre la copia completa y los otros dos tipos de copia (incremental y diferencial) es la información que se almacena en cada iteración del proceso de copia de seguridad[71]:

- Copia total, en este caso se realiza una copia completa y exacta de la información original, independientemente de las copias realizadas anteriormente.

- Copia incremental, en este caso, únicamente se copian los archivos que se hayan añadido o modificado desde la última copia realizada, sea total o incremental.

- Copias diferenciales, en este caso cada vez que se realiza una copia de seguridad, se copian todos los archivos que hayan sido modificados desde la última copia completa.

[71] Una copia de seguridad diferencial no es tan rápida como una incremental, pero es más veloz que una completa; requiere más espacio que una incremental, pero menos que una completa.

En cualquier caso, es necesario hacer pruebas de restauración periódicas, para garantizar que no se producirán problemas en caso de necesitar recuperar nuestra información. Esto es especialmente importante si no se solicitan restauraciones con frecuencia. Los sistemas de copia o los soportes digitales pueden fallar y es fundamental detectarlo antes de que sean necesarios. Además es importante documentar el proceso de respaldo y restauración de copias. Esto permitirá agilizar el proceso de recuperación ante una contingencia.

En caso de que utilicemos almacenamiento en la nube para las copias de seguridad, debemos considerar la posibilidad de que no podamos acceder a la información de manera temporal, por un fallo del servicio o de nuestra conexión a internet.

4.5 Navegación Segura

Elegir un buen navegador es fundamental para garantizar que tus datos se mantengan a salvo. A efecto de promover la navegación segura en internet, se sugiere adoptar las siguientes recomendaciones:

- No guardar contraseñas en el navegador, aunque sea muy cómodo que el navegador tenga tus contraseñas guardadas para entrar rápidamente a todas las páginas que visitas con regularidad, lo cierto es que permitir que los navegadores Web guarden estos datos tan delicados nos pone en una situación de debilidad, ya que cualquier persona que consiga acceder a nuestro ordenador tendría acceso a nuestra información[72].

- Cuando se trabaja desde la Web es recomendable usar el modo Privado o Incógnito para no guardar el historial de navegación, la información introducida en los formularios y borrar al cerrar el navegador los datos de los sitios visitados. Pero recuerda que los sitios Web que visitamos sí guardan información de nuestra visita, nuestro proveedor de internet también guarda constancia de nuestra visita y si descargamos algo, esto no se borra al igual que el historial de descargas, además de las marcas de páginas o favoritos se conservarán al cerrar el navegador.

- Utilizar cifrado de principio a fin (End-toEnd) que utiliza una combinación de algoritmos para identificar al usuario y otros algoritmos que

[72] Es recomendable usar un gestor de contraseñas para almacenar las claves de acceso.

identifican a una conversación para cifrar mensajes y evita que terceros vean la conversación.

- También es posible usar el protocolo mensajería confidencial (Off-The-Record Messaging , OTR), es un protocolo criptográfico que proporciona un cifrado fuerte para conversaciones de mensajería instantánea. La principal motivación debajo de este protocolo es ocultar la identidad de los participantes en la conversación a la vez que se mantenía la confidencialidad de la propia conversación, como si fuera una conversación privada de la vida real.

- No dejar a la vista de otras personas información relevante, como aquélla sensible o claves de acceso, ni documentos o carpetas de trabajo.

- Mantener siempre la computadora, tableta, teléfono celular o cualquier otro dispositivo para el trabajo, en un lugar seguro y con contraseña, a fin de restringir el acceso de personas no autorizadas.

- Al alejarse de los dispositivos de trabajo, es importante bloquear la sesión.

- Mantener cubierta la cámara Web cuando no la estás utilizando, para limitar el acceso que pudieran llegar a tener a ésta aplicaciones o programas no autorizados.

- Sé selectivo con las extensiones y complementos que instalas y usas, a cuantas menos aplicaciones le des acceso a tus datos mejor, ya que pueden mermar el desempeño de tu navegador y es posible que estés cediendo más permisos de los que imaginas.

- Si tu organización facilita los recursos necesarios para el teletrabajo, es indispensable realizar un uso exclusivamente profesional de los medios proporcionados. No se recomienda, en ninguna circunstancia, manipularlos, modificar su configuración, o prestarlos a otras personas.

- Realizar copias de seguridad periódicas -preferentemente encriptadas- de la información para garantizar el acceso a la información almacenada, ya sea personal o de la organización. Así, en caso de que ocurra cualquier incidente de seguridad (robo, pérdida del dispositivo, o avería, etc.), se podrá mantener el acceso a la misma. Proteger con contraseña

los dispositivos donde se almacene información (memorias USB o discos externos) para proteger la información de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

- Ingresar sólo a sitios Web confiables, escribiendo uno mismo la dirección de la página a la que se quiere acceder y evitando utilizar ligas proporcionadas por terceros.
- Conocer y aplicar las funcionalidades de "navegación privada" o "navegación segura", que impiden el almacenamiento del historial en el navegador, así como imágenes, nombres de usuario y contraseñas.
- Cuando se realicen transacciones o intercambio de información sensible, asegurarse de que la dirección de la página Web comience con: "https" (no "http"), lo que contribuye a mantener segura la información transmitida.
- Desactivar la compartición de tu ubicación geográfica, a menos que sea estrictamente necesario.
- Evitar el ingreso de información personal en formularios dudosos. Si te encuentras ante un formulario que solicita información sensible (por ejemplo, nombre de usuario y contraseña), es recomendable verificar la legitimidad del sitio antes de responder.
- Usar cuentas de correo seguro, anónimo y bidireccional como el servicio de ProtonMail. O usar el modo confidencial -en el cual podemos establecer fecha de vencimiento y contraseña para cada correo- al enviar correos desde cuentas Google.
- Usar buscadores que no dejan rastro de nuestras búsquedas en vez del buscador de Google, como pueden ser: DuckDuckGo, Startpage, Yippy, Gibiru, Disconnect Search, Lukol, Metager, entre otros.
- Al terminar de navegar en internet, es importante cerrar la sesión y limpiar el Cache, sobre todo si se utiliza un equipo compartido, para evitar que otras personas tengan acceso a cuentas e información privada.
- Usar el navegador Tor, este provee una red abierta y distribuida que te ayuda a defenderte de una forma de vigilancia en la red que amenaza tu

libertad y privacidad, tus actividades personales y relaciones, además de la seguridad gubernamental. También, te protege redirigiendo tus comunicaciones alrededor de una red distribuida de retransmisores realizados por voluntarios alrededor del mundo: lo cual previene que alguien observe tus comunicaciones a partir de los sitios que visitas, también evita que los sitios que navegas obtengan tu ubicación física.

Seguridad en la Red Una parte importante del trabajo y estudio a distancia es la aplicación de medidas de seguridad de las redes. Es cada vez más común que los usuarios tengan acceso a un Ruteador inalámbrico (Wi-Fi) para conectar sus dispositivos a internet sin necesidad de cables.

Redes Wi-Fi casi todas las redes domésticas comienzan con una red inalámbricas (Wi-Fi), la mayoría de las redes inalámbricas están controladas por el Router de internet o punto de acceso inalámbrico separado y dedicado. Ambas trabajan de la misma manera: transmitiendo señales inalámbricas que permiten que los dispositivos de tu casa se conecten a internet.

Para evitar que usuarios no autorizados se conecten de forma inalámbrica al Ruteador[73] y tengan la posibilidad de acceder a la conexión, e incluso al resto de los dispositivos conectados y a la información que se transmite, es importante mantenerlo actualizado y asegurar que la red Wi-Fi cuente con contraseña robusta (véase sección 4.1) que el usuario debe introducir al conectar por primera vez un dispositivo.

Los Ruteadores ofrecen varios tipos de contraseñas y cifrados (que codifican los datos del usuario, usando un valor o clave secreta y los hace incomprensibles para terceros), como los siguientes:

- Mantener actualizado el Firmware del Router para evitar vulnerabilidades.
- Las redes sin cifrado, o abiertas, son aquéllas que no tienen ninguna contraseña o cifrado y permiten a cualquier usuario conectarse. Estas redes son totalmente inseguras ya que permiten que cualquier dispositivo se conecte al Ruteador sin ningún tipo de seguridad, por lo que

[73] Si no estas seguro de cómo configurar tu dispositivo de acceso a internet, consulta el sitio Web de tu proveedor de servicios de internet, del proveedor para tu Router o punto de acceso inalámbrico.

cualquier usuario podría capturar la información que se transmita a través de dicha conexión.

- El cifrado Wired Equivalent Privacy (WEP, por sus siglas en inglés) es considerado, hoy en día, un sistema poco seguro y no se aconseja su uso ya que, con las herramientas y conocimientos adecuados, se puede llegar a conseguir la clave de acceso a la red Wi-Fi en pocos minutos.

- El cifrado Wi-Fi Protected Access (WPA, por sus siglas en inglés), específicamente en su versión 2 (WPA2) o más actualizada, es considerado seguro y se recomienda comprobar que esté habilitado como parte de las medidas de seguridad de la red. Para comprobarlo, es necesario entrar desde la computadora a las propiedades de la red, para ver el tipo de seguridad de la conexión. Se recomienda tener habilitada alguna de las variantes de WPA2, al menos. Puedes solicitar apoyo a tu proveedor de servicios de internet para más orientación.

Además se recomienda:

- Cambiar las contraseñas predeterminadas en el Ruteador por unas de elección del usuario y distinta a la utilizada para conectarse a la red inalámbrica, utilizando contraseñas robustas (véase sección 4.1).

- Evitar compartir la clave de la red Wi-Fi con otras personas, pues quien tenga acceso a tu red inalámbrica podría tener acceso a todos los dispositivos conectados a ella.

- Cambiar el nombre de la red para que no se identifique el proveedor, pero es preferible ocultar el nombre o SSID, así evitamos que terceros se traten de conectar, pero esto no es una medida de seguridad.

- Habilitar el UPnP (Universal Plug and Play) que permite usar una serie de protocolos de comunicación estandarizados para facilitar la conectividad entre diferentes dispositivos en la red privada, siendo su función principal permitir que los dispositivos soliciten al Router abrir puertos de forma temporal cuando este necesite comunicación con un servidor.

- De ser posible usar filtrado por MAC para asegurar que cada dispositivo que acceda a la red sea el autorizado por ti.

- En caso de conocer los puertos de TCP/IP que usamos, se puede filtrar los no usados para evitar ataques a la red.
- Desactivar el WPS o conexión rápida, si bien pudiese resultar útil, supone una gran amenaza a la seguridad.
- Desactivar el acceso remoto a nuestro Ruteador.

Redes VPN o red privada virtual (Virtual Private Network, VPN) es un servicio mediante el cual se establece una conexión segura a través de internet, entre los usuarios y los servicios o páginas Web de internet a los que éstos acceden.

Si imaginamos el internet como un río en el que fluye el agua (datos e información), la VPN es un tubo, sumergido en el río, que impide ver todo lo que pasa dentro de él, debido a que la conexión entre los dispositivos y el servidor VPN siempre está cifrada (protegida). De esa manera, si alguien interceptara tus comunicaciones, sería incapaz de interpretar la información transmitida.

En algunas ocasiones, las empresas ponen a disposición de sus empleados acceso a través de VPN; de no ser éste el caso o para añadir una capa extra de seguridad a tus comunicaciones personales, las VPN pueden contratarse como servicio (no se recomienda utilizar servicios de VPN gratuitos, pues éstos podrían tener el efecto contrario al deseado de proteger la información). En este sentido, es esencial utilizar un servidor VPN de confianza para el teletrabajo.

Como usuario de una conexión VPN, somos capaces de establecer comunicación con servidores alojados en todo el mundo. ¿Esto qué quiere decir? entre otras cosas, la página Web que visitemos registrará la IP que ofrece el servidor VPN determinado, y pongamos que se encuentra alojado en Estados Unidos. El sitio Web identificará la comunicación como proveniente de este país americano. Y esto ofrece una serie de ventajas como:

- Consumir contenido en Streaming de otros países -por una simple cuestión de derechos de autor-, cada país cuenta con su propio catálogo de contenidos en Streaming, ya sea Netflix o Amazon Prime Video. Incluso existen ciertos servicios exclusivos de un país, imposibles de acceder desde otros. Gracias a una conexión VPN, la orden del servidor para

conectarnos a una de estas plataformas llega desde un país extranjero, por lo que el servicio detectará que estamos en ese país y nos ofrecerá el contenido correspondiente.

- Seguridad en el teletrabajo, gracias a las redes VPN los distintos equipos de una compañía pueden establecer comunicación entre sí, sin necesidad de que estos se encuentren conectados a la misma red. Pueden, incluso, estar en diferentes sucursales de su empresa, situadas en distintos puntos de la geografía mundial. Permitir el acceso a la red local de la empresa desde un sitio externo supone un peligro para los datos almacenados. Sin VPN se pueden establecer contraseñas para acceder a esa red local, pero seguirá siendo susceptible de ataque. A través de una red VPN el acceso y la seguridad de los datos están protegidos.

- Evitar la censura en internet, ciertos países mantienen un control férreo de lo que lo que sus habitantes pueden consumir o no en internet. Por ello, una manera sencilla y segura de saltarse la censura es habilitando en su ordenador una conexión VPN. Por ejemplo, países como China, Corea del Norte o Emiratos Árabes Unidos captan ciertos contenidos que pueden ser accesibles gracias a la conexión VPN.

- Seguridad adicional en nuestra navegación, las conexiones VPN pueden venir acompañadas de un cifrado de la información que se transmite con ellas.

- Protección en descargas P2P, algunos proveedores bloquean la descarga de Torrents a través de programas P2P. Y sin tener en cuenta que podemos estar descargando material legítimo. Gracias a las conexiones VPN esto se podrá evitar.

Redes GPN La misión de las GPN es muy distinta la de las VPN; su nombre (Gamers Private Network) ya da pistas sobre la misma: conectándonos a una no estaremos anonimizando ni cifrando nuestra conexión, sino priorizando la velocidad entre nuestro Router y el servidor del videojuego Online al que estemos accediendo en ese momento.

De hecho, algunos servicios GPN incluso detectan automáticamente a qué videojuego estamos jugando y proceden a enrutarlo automáticamente (y a priorizarlo sobre otras aplicaciones que se estén ejecutando en ese momento).

¿Y cuál es el sentido de eso? Muy sencillo: reducir la latencia de la conexión, así como el Ping, lo que evitará la pérdida de paquetes... y repercutirá en pro de la experiencia de juego; y puede resultar clave durante la partida, a la hora de mejorar la velocidad de reacción de nuestro 'avatar'.

Está, la aceleración de la conexión, es la meta principal del uso de una GPN. Aunque, como en el caso del VPN, existe otra función extra que ambos comparten: conectándonos desde una GPN, resulta posible acceder a juegos o DLCs que aún no están disponibles en nuestro país (o peor, que no está previsto que lo estén nunca).

Pese a esta separación entre VPNs y GPNs, es relativamente habitual que los proveedores de herramientas VPN ofrezcan igualmente servicios GPN, muchas veces integrándolos en la misma aplicación.

Prevención de Ataques a una Red para mantener un cierto grado de protección de la información conectada a la red, las organizaciones, entidades y personas en general, deben comprender que su seguridad, y las formas en que esta se trata de vulnerar, mejoran constantemente; por tanto, lo principal y primero es entender cómo pueden sucederse estos ataques y en qué consisten dichas amenazas, con el fin de poder remediarlas de la mejor forma posible.

Existen diferentes formas efectivas para lidiar y mitigar los ataques que pueden suceder en una red. En función del tipo de ataque, algunas de ellas son:

- Para prevenir Malware, Adware y Spyware: instalar en los dispositivos un Software antivirus como primera protección, mantenerlo actualizado como segunda, y realizar escaneos periódicos como tercera. Ejecutar parches de seguridad en los sistemas operativos que se empleen, realizar copias de seguridad de los datos y emplear contraseñas diferentes y bien formadas para cada servicio al que se accede, configurar adecuadamente la seguridad de los navegadores y no descargar de la red aplicaciones o archivos de procedencia desconocida.

- Para prevenir Ransomware: La primera recomendación es tener actualizado el sistema operativo y todas las soluciones de seguridad, así como el antivirus y el cortafuegos personal habilitado (Firewall); evitar los accesos administrativos desde fuera de la entidad, y en caso necesario, permitirlos sólo mediante protocolos seguros. Activar la visua-lización de

las extensiones de los ficheros para evitar ejecución de código dañino camuflado como ficheros legítimos no ejecutables, deshabilitar las macros en los documentos, educar a los usuarios de la red para reconocer amenazas antes de abrir archivos adjuntos enviados por correo electrónico, y realizar copias periódicas de respaldo de información para sistemas críticos.

- Para prevenir el Escaneo de Puertos: una forma efectiva es cerrar los puertos o servicios que no se utilizan en los sistemas, siempre que sea posible, emplear puertos no conocidos para determinadas aplicaciones (y no los configurados por defecto), tener configurado un cortafuegos (Firewall), y silenciar o desinformar las respuestas a encuestas de puertos.

- Para prevenir el Phishing: se recomienda a los usuarios de la red ir despacio ante cada acción, sin importar la urgencia que se emplee en los mensajes que se reciben; investigar los hechos y sospechar de cualquier comunicación no solicitada o desconocida. Rechazar y no responder ninguna solicitud de información confidencial como contraseñas o datos de tarjetas de crédito, así como nunca descargar ni ejecutar archivos adjuntos de personas desconocidas.

- Para prevenir ataques de Botnets: es necesario cambiar regularmente las contraseñas de acceso, incluido el Router de conexión; mantener actualizado el sistema operativo y el antivirus instalado, evitar realizar descargas P2P o vía Torrent porque, en muchas ocasiones, es la principal vía de entrada para estas infecciones, así como limitar el acceso a sitios cuya seguridad resulte sospechosa.

- Para prevenir la Denegación de Servicios (DoS): se deben bloquear direcciones IP que no se empleen, así como deshabilitar puertos y servicios de red innecesarios, aplicar filtros de enrutamiento, permitiendo solo el acceso al tráfico deseado, realizar una efectiva política de contraseñas, así como establecer la cantidad de ancho de banda a emplear por los usuarios.

- Para prevenir ataques de intermediario (Man In The Middle, MITM): la variante más adecuada es cifrar el tráfico que se envía por redes abiertas. Para ello se utilizan las redes virtuales privadas (VPN) y se

emplea para los documentos la Infraestructura de las Llaves Públicas (Public key Infrastructure, PKI), Certificados Digitales, y una Entidad Certificadora, lo que contribuye a proteger los documentos enviados y confirmar la identidad de los usuarios mediante el cifrado de los mensajes. Una PKI establece un esquema de confianza en el cual ambas partes de una comunicación electrónica confían en un ente emisor para que verifique y confirme la identidad de ambas.

4.6 Mensajería Instantánea

La agencia de ciberseguridad estadounidense, CISA, ha publicado este 2024 una guía de mejores prácticas para las comunicaciones móviles, donde insta a funcionarios gubernamentales a usar las tecnologías de cifrado de extremo a extremo y en concreto, en aplicaciones de mensajería instantánea, las más seguras como Signal.

La guía se ha elaborado en respuesta a la ola de violaciones de seguridad en operadoras de telecomunicaciones de docenas de países, incluidas ocho en Estados Unidos. La CISA y el FBI confirmaron estas infracciones a finales de octubre, después de conocerse que Salt Typhoon, un grupo de ciberdelincuentes presuntamente financiados por el estado chino y conocido bajo distintos nombres desde al menos 2019, hubiera atacado a grandes telecos como T-Mobile, AT&T, Verizon y Lumen Technologies. Aunque no está claro el momento en que se produjeron las infracciones, se informó que los atacantes tuvieron acceso a los datos durante «meses o más».

Aunque las directrices mencionadas por la CISA se aplican a individuos muy específicos que probablemente posean información de interés para los ciberespías chinos, las medidas pueden ayudar a cualquier persona que quiera proteger sus datos e información de los piratas informáticos que violan con éxito la seguridad de sus operadores móviles.

Y el campo de acción es total: «Debe asumirse que todas las comunicaciones entre dispositivos móviles, incluidos los dispositivos gubernamentales, los personales y los servicios de Internet, corren el riesgo de ser interceptados o manipulados«, asegura la agencia de ciberseguridad estadounidense.

La recomendación (encarecida) del uso del cifrado de extremo a extremo es un gran cambio de paradigma frente a otros tiempos donde algunas agencias y reguladores solicitaban precisamente lo contrario, un debilitamiento de estas tecnologías citando la 'seguridad nacional'.

Los expertos en seguridad y las organizaciones que velan por los derechos en Internet, consideraron que la idea de recortar la seguridad de los sistemas de cifrado con el socorrido argumento de la «seguridad» era un auténtico disparate. Ya no solo es que un sistema democrático no pudiera admitir que la «delincuencia» fuera una excusa para recortar derechos fundamentales, es que de los sistemas de cifrado depende la ciberseguridad mundial, Internet y servicios tan delicados como el comercio electrónico o la banca en línea.

En cuanto al uso de «puertas traseras» con la que romper el cifrado de extremo a extremo por las autoridades, no se consideran seguras y con total seguridad terminarían llegando a los ciberdelincuentes que las usarían en un modelo terrible para la seguridad mundial. Y es que debilitar los sistemas de cifrado destruiría la protección de todos en lugar de investigar a los sospechosos, socavando décadas de avances en seguridad que protegen a clientes y ciudadanos.

No es fácil encontrar el equilibrio en estas cuestiones, siempre delicadas, donde también hay que facilitar la batalla de los estados, los servicios de inteligencia y sus cuerpos de seguridad contra los 'malos', pero la opinión de la agencia de ciberseguridad estadounidense a favor de las tecnologías de cifrado es clara: «CISA insta encarecidamente a las personas altamente vulnerables a que revisen y apliquen de inmediato las mejores prácticas proporcionadas en la guía para proteger las comunicaciones móviles, incluido el uso consistente del cifrado de extremo a extremo«, dicen desde la agencia.

Signal, la recomendada en mensajería instantánea en la guía de buenas prácticas, CISA recomienda usar una aplicación de mensajería segura y nombra específicamente a Signal para la comunicación móvil en múltiples plataformas móviles (iOS, Android) y de escritorio (macOS, Windows y Linux).

Aunque hay otras alternativas (incluso más seguras), Signal es la mejor opción entre el Software gratuito. Ofrece chat de video, voz y texto, llamadas de voz y vídeo con cifrado de extremo a extremo, así como transferencias seguras de archivos y fotos. Funciona bajo el protocolo Signal Messaging Protocol, ampliamente reconocido como el protocolo de mensajería más seguro disponible y es un desarrollo Open Source, lo que significa que su código está disponible en línea para escrutinio público y cualquier cuestión de privacidad o fallo de seguridad puede ser verificado por expertos.

A pesar de estar alejada del millonario número de usuarios de Telegram o

WhatsApp, Signal es el gran nombre actualmente en mensajería instantánea y no es raro que la CISA la recomiende, si bien hay otras incluso más seguras como Threema o con enfoque más empresarial como Wire.

La agencia también recomienda utilizar la autenticación multifactor (MFA) resistente a la suplantación de identidad, junto con claves de seguridad FIDO basadas en Hardware (por ejemplo, Yubico o Google Titan) o claves de acceso para proteger las cuentas de Microsoft, Apple y Google. Siempre que sea posible, también se deben habilitar opciones como el programa de Protección avanzada (APP) de Google o el modo de bloqueo de Apple para protegerse contra el secuestro de cuentas y los ataques de suplantación de identidad.

Además, CISA recomienda evitar la MFA basada en SMS (demostrada insegura), utilizar un administrador de contraseñas para almacenar y proteger las contraseñas de los atacantes y configurar un PIN o código de acceso de la compañía telefónica para operaciones sensibles como portar su número de teléfono y bloquear los intentos de intercambio de SIM.

4.7 Banca en Línea Segura

El uso de la banca en línea es una gran alternativa para todos los usuarios de dichos servicios, pero el acceso a las aplicaciones bancarias debe ser usando un navegador Web seguro o por medio de las aplicaciones del banco desarrolladas para dispositivos móviles, en ambos casos es necesario usarlas en un dispositivo de confianza, cifrado, con contraseña segura para el acceso (véase sección 4.1), el sistema operativo actualizado, usando las medidas básicas de protección y con un mínimo de aplicaciones instaladas para evitar Malware, además se sugiere adoptar las siguientes recomendaciones:

- Solicitar al banco que nos envíe alertas de todas las transacciones de nuestras cuentas y mantengamos estas monitoreadas de actividad no autorizada.
- Cuando se deba tener acceso a banca en línea es necesario conectarse usando redes seguras en las que uno confié, nunca desde redes públicas
- Cuando se deba tener acceso a banca en línea desde la Web es recomendable usar el modo Privado o Incógnito y no guardar contraseñas en el navegador.

- Ingresar sólo a sitios Web confiables, escribiendo uno mismo la dirección de la página a la que se quiere acceder y evitando utilizar ligas proporcionadas por terceros y asegurarse de que la dirección de la página Web comience con: "https" (no "http").
- Usar en la medida de posible contraseñas seguras del mayor tamaño permitido por la aplicación bancaria.
- No dejar a la vista de otras personas información relevante, como aquélla sensible o claves de acceso, ni documentos o carpetas de trabajo.
- Mantener siempre la computadora, tableta o teléfono inteligente usado para acceder a la banca en línea en un lugar seguro y con contraseña segura, a fin de restringir el acceso de personas no autorizadas.
- Al alejarse de los dispositivos de trabajo, es importante cerrar la sesión bancaria y bloquear la sesión del usuario.
- Ser selectivo con las extensiones y complementos que instalas y usas, a cuantas menos aplicaciones le des acceso a tus datos mejor, ya que pueden mermar el desempeño de tu navegador y es posible que estés cediendo más permisos de los que imaginas.
- Al terminar de navegar en internet, es importante cerrar la sesión y limpiar el Cache, sobre todo si se utiliza un equipo compartido, para evitar que otras personas tengan acceso a nuestras cuentas bancarias.

4.8 Uso Seguro de las Herramientas de la Nube

La nube permite almacenar y administrar datos, así como ejecutar aplicaciones en línea, entre muchas otras funciones. Con relación al almacenamiento, la nube permite acceder a archivos y datos desde cualquier dispositivo conectado a internet; es decir, la información está disponible en cualquier lugar en el que te encuentres y siempre que la necesites.

Para hacer uso de los servicios de la nube de manera segura y evitar el robo o mala utilización de la información almacenada, es conveniente tener en mente las siguientes recomendaciones:

- Tener conocimiento de las condiciones de uso y las políticas de privacidad antes de utilizar cualquier servicio en la nube.
- Utilizar servicios de almacenamiento que cuenten con cifrado "https" y certificado de seguridad. Esto lo puedes verificar en la barra de direcciones de tu navegador de internet.
- No subir a la nube información sensible con acceso público o abierto. Se recomienda utilizar herramientas de cifrado, como es el uso de carpetas con contraseña y acceso restringido.
- Verificar periódicamente los archivos y carpetas que tenemos compartidos desde nuestra cuenta, a fin de deshabilitar los enlaces y acceso de terceros que ya no sean necesarios.
- Utilizar contraseñas robustas para acceder al servicio y, preferentemente, activar el doble factor de autenticación o verificación en dos pasos.
- Realizar periódicamente un respaldo de la información almacenada en la nube en otro tipo de dispositivo, por ejemplo, en un disco duro externo debidamente protegido por contraseña (véase sección 4.3). De esa manera, se mantiene el acceso a la información en caso de cualquier contratiempo, como una conexión limitada a internet.
- Cerrar la sesión de la nube al concluir las actividades que se estén realizando.

4.9 Protección de Teléfonos, Tabletas y Computadoras

Estos dispositivos están omnipresentes en nuestra vida, además pueden almacenar mucha más información de la que nos imaginamos y muchos de nosotros los usamos para acceder a casi toda nuestra información digital desde ellos. Por tanto, necesitan protegerse activamente para evitar que el contenido que almacenan y al que tienen acceso termine en manos de terceras personas. En ellos se guardan todo tipo de datos personales, mensajes, imágenes y vídeos

en los que aparecen los usuarios, amigos y otras personas. A veces incluso se puede haber recibido o grabado contenido íntimo o de connotación sexual[74].

Hay que hacer notar que varias empresas tecnológicas (en conjunción con las leyes de diversos países) en su lucha contra el terrorismo y por la protección de los jóvenes han anunciado nuevas funciones a su Software para la revisión de mensajes y escaneo de imágenes almacenados y enviados en busca de material de abuso y explotación sexual infantil frente a los extraños que utilizan herramientas de comunicación para reclutarlos y explotarlos. Si bien los objetivos son loables y no cabe duda que no existen respuestas fáciles cuando se trata de poner en peligro a los niños, pero rompe la promesa de cifrado de dispositivos y de mensajes de extremo a extremo, inevitablemente se abre la puerta a otros daños colaterales.

No olvidemos que cualquier método de almacenaje de información digital puede sufrir filtraciones o ataques informáticos, pero los dispositivos móviles son aún más vulnerables. Pueden extraviarse, también pueden ser robados en diversas situaciones o, simplemente, ser interceptados en un momento de despiste. Por ello estos son algunos de los hábitos que debemos practicar a diario para mejorar la protección del dispositivo y nuestros datos:

- Todos los dispositivos móviles y tarjetas de respaldo extraíbles deben ser cifrados y se debe usar una contraseña robusta para el acceso al mismo (véase sección 4.1), es decir, utilizar una combinación compleja -de al menos 15 caracteres- de letras mayúsculas, minúsculas, números y símbolos es siempre la mejor opción. Además, es imprescindible no confiarla a sus amistades y cambiarla siempre que tengan dudas de su fiabilidad.

- Es fundamental que se comprenda que toda la información que guardan en el dispositivo es susceptible de caer en manos de terceras personas. Por eso, lo ideal es que no guarden imágenes, vídeos o datos de carácter sensible. Es preferible que revisen periódicamente sus archivos, eliminen de forma eficaz aquello de lo que puedan prescindir y, en el caso

[74] En el caso de los adolescentes no siempre son conscientes del riesgo que supone producirlo o guardarlo, Pero, en cualquier caso, requiere una protección especial, y como adultos podemos mostrarles la importancia de proteger estos contenidos.

Este tipo de contenido es extremadamente sensible y, de hecho, cuando se trata de imágenes o vídeos en los que aparecen menores de edad ni siquiera es legal almacenarlo en ningún tipo de formato.

de querer guardar algunos contenidos, los almacenen en otros dispositivos más seguros, como un disco duro externo cifrado (véase sección 4.3) que mantengan en casa. Cuanta menos información lleven en su dispositivo, menor riesgo.

- Mantener siempre actualizados nuestros dispositivos y en caso necesario usar alguna aplicación para seguridad y protección de dispositivos móviles.

- Cualquier dispositivo ofrece un sistema de bloqueo para que nadie que no sea el usuario pueda acceder a él. En el caso de móviles y tabletas, tienen diferentes alternativas, como usar su huella dactilar, un sistema de reconocimiento facial, un código PIN, una contraseña o un patrón. Cualquier opción es buena, pero hay que tener en cuenta que un patrón o un código PIN siempre son más fáciles de observar y memorizar por otras personas. Obviamente, esta función pierde su eficacia si no se acostumbran a bloquear el dispositivo siempre que no lo estén utilizando.

- Algunos servicios de internet, como cuentas de correo o redes sociales, ofrecen un sistema combinado de autenticación. De esta forma, además de solicitar la contraseña para acceder, utilizan un segundo paso para comprobar la identidad del usuario. Puede ser un código que llegue a su teléfono móvil, por ejemplo, y es muy útil contra el robo de contraseñas. Para ponernos en situación, si alguien averigua la clave de acceso a su cuenta de Instagram no podrá acceder porque también necesitará disponer del dispositivo para ver el código de verificación.

- Siempre es una buena costumbre cerrar la sesión de cada servicio al concluir su uso. Por ejemplo, si se entra en redes sociales o en su cuenta de correo en el ordenador público, es fundamental que cierren la sesión y limpiar el Cache antes de irse, comprobando que su contraseña no ha quedado guardada.

- Hoy en día todos los servicios digitales incorporan opciones de seguridad y privacidad que se han diseñado para proteger nuestra información. Una buena práctica es revisar la configuración de cada aplicación o servicio que se utilice, personalizando todas aquellas funciones que les sean de utilidad. Así, se pueden establecer cuentas de redes sociales como privadas o revisar los permisos que otorgan a cada aplicación.

- Existen muchas más funciones que pueden ser útiles para salvaguardar todas esos datos, imágenes y vídeos que se guardan en los dispositivos. Todo es cuestión de investigar y buscar soluciones siempre que sientan que su información es vulnerable. Por ejemplo, pueden bloquear la galería de su móvil o el explorador de archivos, de forma que sea necesario utilizar su huella para acceder. También pueden crear listas de amistades en las redes sociales para que las publicaciones sean más personales y no lleguen a todos los seguidores.

- Activar la función de búsqueda y bloqueo de dispositivo frente a pérdidas o robos. Cada vez hay más opciones de seguridad disponibles, solo hay que motivar su uso en la prevención de riesgos.

- Activar el Wi-Fi y Bluetooth sólo cuando se usen, de esta forma se minimiza la posibilidad que un usuario malintencionado intente conectarse a nuestro dispositivo.

- Es posible poner un código de acceso en su tarjeta SIM, esto puede protegerla de la suplantación de SIM. La configuración de este código se puede hacer en un iPhone yendo a Configuración > Celular > PIN de SIM. Ingrese su PIN existente para habilitar el bloqueo. Los usuarios de Android pueden ir a Configuración > Seguridad > Bloqueo de tarjeta SIM. Aquí puede habilitar la opción para bloquear su SIM.

- Se debe evitar el uso de puertos de carga USB no confiables, como los de energía públicos, ya que ellos se pueden Hackear, y el ciberdelincuente puede instalar, grabar datos, tomar video o sacar datos de nuestros dispositivos móviles. Si se hará uso de este tipo de servicios, es recomendable adquirir un dispositivo del tipo PortaPow de carga rápida con adaptador USB que inhabilitan los pines de datos permitiendo sólo la carga del dispositivo.

- Al desechar el dispositivo, es necesario reiniciarlo para borrar toda la información que pudiese contener, además se debe retirar la tarjeta SIM y destruirse.

4.10 Escaneo de Códigos QR de Forma Segura

Los códigos QR[75] cada vez están más presentes en nuestras vidas, sin embargo, éstos no están exentos de riesgos de seguridad, riesgos de los que muchos de nosotros no somos conscientes.

Si bien los códigos QR son muy prácticos para compartir desde la contraseña del WiFi, tu número de WhatsApp o la cuenta de Instagram de alguien a quien acabas de conocer. Y poco a poco se va abriendo paso en escaparates, publicidad o puertas de establecimientos para que puedas descargar sus aplicaciones o entrar en sus páginas Web. Y qué decir de restaurantes y bares que ofrecen su carta o menú en formato digital a través de un código QR que puedes escanear cómodamente con tu teléfono móvil.

Los QR son Menos Transparentes que una URL comencemos por lo más obvio, es relativamente fácil distinguir una URL maliciosa de una legítima, pero no ocurre lo mismo con los con los enlaces cortos y menos con los QR, lo que facilita que seamos remitidos a Webs de Phising o con Malware, a está técnica se le conoce como Quishing. Si bien, los códigos QR se pueden usar para bien, también para mal. Es decir, uno de los problemas de seguridad de los códigos QR es que no sabes realmente a dónde te llevará ese código hasta que no lo escaneas. Eso significa que tienes que pulsar en el enlace para verlo en tu navegador. Y ahí ver si lo que estás viendo es la página de una tienda de ropa o una falsa página que quiere robar tus datos o engañarte para que introduzcas tu tarjeta de crédito.

Escanear códigos QR y seguridad decíamos que el código QR es un código que tiene forma de cuadrado con píxeles negros y que sirve para compartir información. Esta información puede ser un enlace a una página Web, un mensaje de texto, una imagen colgada en internet, un número de teléfono, etc. Se utilizan códigos QR para realizar pagos, para llevar encima Boletos de avión, para consultar la carta de un restaurante, para comprar

[75] Un código QR, nomenclatura para Quick Response o Respuesta Rápida, es una imagen escaneable de una matriz de dos dimensiones que pertenece a la familia de los códigos de barras que podríamos encontrar en otros productos, diseñado inicialmente en 1994 para la industria automotriz en Japón. Estos códigos son capaces de almacenar información hasta un total de 7089 caracteres numéricos o 4296 caracteres alfanuméricos en la versión 40 de estos códigos.

Online, para ver un vídeo publicitado en un cartel en la calle o en una revista o diario... hay muchas posibilidades.

Además, escanear códigos QR no tiene ningún misterio. Tanto Android como iOS integran en su aplicación de cámara la detección de códigos de este tipo cuando los enfocas con la cámara del teléfono. Así, al detectarlo te muestra el enlace o contenido oculto para que lo abras en tu navegador o lo copies al portapapeles del dispositivo.

No Entendemos qué Puede Abrir un Código QR otro problema es que los usuarios no terminan de comprender qué es lo que pueden hacer los códigos QR, mientras que el 67% piensa (correctamente) que pueden abrir URLs, sólo una tercera parte de ellos es consciente de que eso permite también realizar toda una serie de acciones más allá de abrir una página Web, como:

- Escribir un correo electrónico o un mensaje SMS.
- Añadir un contacto a tu agenda.
- Añadir un evento a tu calendario.
- Añadir credenciales de acceso a una red WiFi.
- Realizar un pago Online.
- Iniciar una llamada telefónica.
- Enviar información sobre tu localización a una app.
- Empezar a seguir a alguien en redes sociales.
- Te llevará a descargar un Malware.

Aunque todas éstas actividades son en cierto modo lícitas, pueden engendrar una gran brecha de seguridad en nuestros dispositivos móviles.

Consejos para no caer en estafas con QR para evitar escanear códigos QR dañinos hay varias cosas que podemos hacer antes de que nos encontremos con uno. Básicamente, se trata de ser precavidos como ocurre con otros métodos de engaño relacionados con internet o con tu Smartphone.

Para empezar, tener siempre tus aplicaciones y tu sistema operativo actualizados. Así evitarás que una aplicación falsa o dañina aproveche un agujero de seguridad para hacerse con el contenido de tu teléfono.

En segundo lugar, la manera más directa de evitar un código QR falso es no pulsar en el enlace cuando veas la vista previa. De la misma manera que no debes pulsar en un enlace enviado por un SMS desconocido, no debes entrar en enlaces que no conozcas. Si has escaneado el código QR de un determinado establecimiento pero el enlace no se parece nada a ese negocio o tiene un dominio extraño o genérico, evita abrirlo en tu navegador.

Tanto si vas a escanear códigos QR con la cámara directamente como si utilizas una aplicación específica, verás la vista previa de lo que esconde el código QR. Si es así, puedes buscar el enlace en internet y ver si ya ha sido denunciado.

Una manera de asegurarte de que un enlace es seguro, es que emplee el protocolo HTTPS en vez del clásico HTTP. Si es así, sabrás que esa página es de fiar, si bien esto no garantiza al 100% que la página sea real o una réplica.

Y, para terminar, un consejo importante. Para realizar compras Online o hacer pagos por medios digitales, procura hacerlo desde las aplicaciones oficiales y/o las páginas oficiales. No compartas datos bancarios o información de pago en enlaces abiertos con un código QR.´

Analizar los enlaces tras escanear códigos QR Para quedarte tranquilo y comprobar si lo que esconde un código QR es seguro o hay detrás una página o aplicación maliciosa, puedes escanear el enlace que aparece al igual que hacemos con los enlaces acortados o con los archivos que descargamos de fuentes desconocidas. Gracias a las páginas de análisis Online como VirusTotal y similares, puedes asegurarte de que un enlace es de fiar o si esconde algo. Y si usas Android, tienes a tu disposición una App no oficial pero recomendada por ellos mismos. La App analiza tus aplicaciones instaladas además de archivos y enlaces que pidas analizar.

Si usas iPhone, verás la vista previa del enlace antes de abrirlo. En Android, al haber más peligro con la instalación de aplicaciones falsas y Malware, proliferan en Google Play aplicaciones de seguridad para escanear códigos QR de forma segura. Así podrás escanear esos códigos y, desde la misma App, saber si son o no de fiar.

4.11 Uso de Redes Sociales Responsablemente

El uso generalizado de las redes sociales entraña algunos riesgos que, siguiendo recomendaciones básicas, se pueden evitar. Como cualquier comunidad frecuentada por miles de usuarios (o, como sucede a veces con las redes sociales, por millones), se deben conocer los mecanismos de control y de seguridad para poder utilizarlos con fiabilidad para mantener nuestra privacidad y es por eso que el usuario tiene que ser especialmente cuidadoso con el uso que hace de la red social, a continuación daremos algunas recomendaciones:

- La gente tiende a inundar de información mientras completa los perfiles en redes sociales. Hay que tener en cuenta que no estamos ante una entrevista de trabajo o que sólo nuestros amigos lo van a leer. No necesitamos informar de todo y a todos, y menos con información sensible. Los expertos creen que revelar demasiada información personal crea una grieta de seguridad. Los atacantes usan información personal como la fecha de nacimiento, el nombre de los miembros de la familia, los números de teléfono, la dirección física, etc. Todo ello para ejecutar múltiples iteraciones para descifrar las contraseñas. Por ello, cuanta menos información pongamos, mejor.

- A menudo publicamos notas o mensajes en el muro de un amigo. Esto también es visible para otros usuarios de Facebook o de la red social que sea. No existe una fórmula para decidir qué es seguro publicar en público y qué no, pero hay que usar el sentido común. Algunas cosas deben mantenerse entre amigos o familiares. Publicar cierta información en muros públicos pone en riesgo no solo a nosotros mismos sino a la privacidad de nuestros amigos.

- Se dice que una foto vale más que mil palabras. En el caso de las redes sociales incluso más. Además si subimos imágenes con una leyenda informativa, nos pone aún más en riesgo. Estamos dando información sobre nuestros hábitos, nuestros movimientos, a posibles atacantes. Es un aspecto importante para mantener la seguridad en redes sociales.

- Hay que asegurarse de que nuestro contenido en las redes sociales sea visible solo para amigos y familiares. Podemos crear listas de tipos de amigos y personalizar la visibilidad de cada publicación. No todo debe

estar visible para esa persona que trabajó con nosotros durante unas semanas hace unos años, por poner un ejemplo. Puede que haya cosas que no queramos compartir con todos los contactos.

- El GPS es una característica común en todos los teléfonos inteligentes en la actualidad. Además de ayudarnos mientras pasamos por una ciudad desconocida, el GPS también se utiliza para el geoetiquetado. Significa que podemos adjuntar información de ubicación a cualquier contenido multimedia que enviemos o recibamos. Twitter, Facebook e Instagram usan esta característica extensivamente para ayudar a los usuarios a marcar la ubicación donde se hizo una foto, y ayudar a que el perfil sea más «social». Los atacantes cibernéticos pueden interpretar fácilmente información como nuestro estado económico, estilo de vida, lugares frecuentes y la rutina diaria a través de los medios con etiquetas geográficas.

- Una de las maneras más elementales de fortalecer nuestra cuenta de redes sociales es crear una contraseña robusta (véase sección 4.1), es decir, utilizar una combinación compleja -de al menos 15 caracteres- de letras mayúsculas, minúsculas, números y símbolos es siempre la mejor opción. Además, es imprescindible no confiarla a sus amistades y cambiarla siempre que tengan dudas de su fiabilidad.

- Guardar contraseñas en el dispositivo es una práctica muy habitual. Simplemente la abrimos y ya está, sin necesidad de tener que poner la clave cada vez que la usamos. Sin embargo, esto no es un buen método. Si alguien accede físicamente a nuestro teléfono o al ordenador, podría entrar sin problemas a nuestras cuentas. Lo más recomendable es no guardar contraseñas.

- En las redes sociales debemos de tener cuidado con los Links que nos llegan. Incluso si éstos proceden de algún amigo. Hay que fijarse bien en el enlace. En lo que contiene. Muchas veces puede ser una trampa. Nuestro contacto lo hace de forma inconsciente, claro. Pero se trata realmente de un Malware.

- Algo que no puede faltar es contar con programas y herramientas de seguridad. Pero esto no se extiende únicamente a la seguridad en redes sociales, sino a cualquier acción que hagamos en internet. Siempre

tenemos que tener algún antivirus instalado. Así podremos hacer frente a posibles amenazas que pongan en riesgo el buen funcionamiento de nuestro equipo.

- En una red social lo normal es que cada usuario se identifique con su nombre y apellido real y que aporte datos personales, como si estudia o trabaja, con quién se relaciona o en qué ciudad vive. También es muy frecuente subir fotografías personales donde el usuario es perfectamente identificable. Esto hace que su exposición pública sea mucho mayor que antes, esto implica la pérdida del anonimato algo que antes era común y habitual en internet.

- En las redes sociales, una vez que se pulsa el botón de "publicar", esa información es enviada a los contactos del usuario. Eso significa que si más adelante el usuario se arrepiente de lo dicho, publicado o mostrado y trata de borrarlo, solo conseguirá eliminarlo de su propio perfil, pero no de las cuentas de todos sus amigos.

- Es muy común que de forma periódica aparezcan solicitudes de amistad en el perfil de cada usuario, por parte de personas que en realidad no se conocen. Muchas veces el acto de aceptar una de esas solicitudes es tan automático que no se vigila si se está admitiendo a una persona conocida o no. Los amigos se pueden contar con los dedos de las manos (con una suele ser suficiente) mientras que lo que encontramos en las redes sociales son conocidos con los que debemos mantener la correspondiente distancia.

- Una red social es un lugar muy atractivo para estar; mientras más amigos se tienen, más novedades aparecen de forma constante en la página de cada uno, creándose un ciclo de interacciones que no tiene un final concreto. Eso hace que algunas veces el usuario sienta la necesidad de estar siempre pendiente y atento a su red social, dándose casos esporádicos y extremos de dependencia total a su red.

- Quizás lo más importante de estos consejos para mantener la seguridad en redes sociales es el sentido común. La gran mayoría del Malware necesita la interacción del usuario para ejecutarse. Debemos estar siempre alerta y usar el sentido común.

Acuerdos de Privacidad La lectura de los acuerdos de privacidad orientará al usuario sobre qué datos se comparten o no, y también se ofrece la opción de seleccionar o anular las opciones de privacidad, seguridad o administrativas escogidas para proteger la cuenta y el dispositivo.

Si de verdad leyéramos los términos y condiciones de uso de plataformas Online, tardaríamos (con una velocidad de 240 palabras por minuto) aproximadamente (seleccionadas con datos de abril 2020):

- Microsoft 1:03:30 s (15,260 palabras)
- Spotify 35:48 s (8,600 palabras)
- Tik Tok 31:24 s (7,459 palabras)
- Apple 30:30 s (7,314 palabras)
- Zoom 30:12 s (7,243 palabras)
- Tinder 25:54 s (6,215 palabras)
- Uber 25:36 s (5,658 palabras)
- Twitter 25:30 s (5,633 palabras)
- LinkedIn 18:06 s (4,346 palabras)
- Facebook 17:12 s (4,132 palabras)
- Amazon 14:12 s (3,416 palabras)
- YouTube 13:42 s (3,308 palabras
- Netflix 11:00 s (2,628 palabras)
- Instagram 9:42 s (2,451 palabras)

Estas son algunas recomendaciones generales a tener en cuenta para administrar mejor la configuración de privacidad en una cuenta de redes sociales:

- Selecciona quién tiene acceso de visualización a la actividad en redes sociales pasada, presente y futura (por ejemplo, Tuits, Me gusta, etc.).

- Revisa qué contenido se le puede agregar (es decir, etiquetar) a una cuenta cuando otras personas suban o publiquen contenido.
- Revisa, comprende y define la audiencia con la que se puede compartir contenido.
- Revisa, comprende y determina los formularios a través de los cuales otros usuarios pueden encontrar y conectarse con tu cuenta.
- Revisa, comprende y determina la cantidad de información personal que se incluye al bloguear o publicar información en línea.
- Monitorea periódicamente la seguridad y la información de inicio de sesión de las cuentas y revisa la probabilidad de que se esté realizando alguna actividad sospechosa.
- Selecciona una copia de seguridad confiable, que pueda detectar o recibir alertas de alguna actividad sospechosa.
- Monitorea si y qué aplicaciones pueden acceder a alguno de tus datos y/o información en redes sociales, especialmente en segundo plano.
- Ten en cuenta las implicaciones de incluir la ubicación al publicar contenido en línea.
- Configura una autenticación de dos factores para iniciar sesión.
- Revisa la política de privacidad de la plataforma para saber qué datos recopilan los servicios, con quién se comparten y selecciona tus preferencias en estos dos temas.

Al registrarte en una cuenta de redes sociales, por defecto, toda la información anotada en un perfil se hace pública, lo que significa que cualquier persona puede acceder al contenido que hayas registrado en una cuenta. Sin embargo, las necesidades y preferencias de privacidad varían de persona a persona. Mientras que algunos usuarios prefieren tener una mayor exposición y así poder promocionar su contenido en redes sociales, otros prefieren incluir muy poca o ninguna información.

Para lograr una mayor protección del usuario y su información, es importante evaluar en qué medida la persona está dispuesta a incluir información personal en su perfil. Por consiguiente, ten en cuenta lo siguiente al:

- Seleccionar un nombre de usuario: el nombre de usuario es el "nombre digital" que una persona se asigna a sí misma o a su organización para ser identificada en línea. Si existe la preferencia de no ser fácilmente identificada en ninguna plataforma, pero poder continuar usando estas redes, la persona puede asignar y usar un seudónimo que puede estar relacionado o no con esa persona. Además, la persona puede cambiar su nombre de usuario en cualquier momento simplemente ingresando a la configuración de su (s) cuenta (s). El nombre de usuario no tiene que ser coherente en todas las redes sociales; estas pueden variar según las preferencias en cada una.

- Incluir una imagen en la cuenta: el usuario tiene la opción de personalizar una cuenta con la inclusión de una foto del perfil. Cuando un usuario prefiere no ser identificado, se sugiere elegir una imagen en la que no pueda ser identificado y cambiarla cuando sea necesario. Ten en cuenta que cuando se usa la misma imagen en todas las redes sociales, la simple búsqueda de imágenes puede llevar a otras cuentas.

- Incluir una ubicación: cuando se activan los servicios de ubicación en la plataforma de redes sociales, estos les permiten a los usuarios rastrear el origen de cualquier actividad de medios en línea. Es importante tener en cuenta que una vez que se activa esta función, permanecerá activa hasta que se elija deshabilitarla en la configuración de privacidad. A pesar de que se permitía que esta característica estuviera activa en el pasado, las plataformas tienen la funcionalidad de deshabilitar la ubicación de cualquier contenido que se haya publicado en sus cuentas.

Sin embargo, aunque un usuario active o desactive la función de compartir la ubicación, potencialmente, la ubicación de un usuario podrá ser descubierta por el contenido que comparta o las imágenes que haya elegido para compartir.

4.12 Seguridad en Videoconferencias

También conocidas como teleconferencias o videollamadas[76] se han convertido en una herramienta indispensable para el trabajo, estudio y placer de

[76] Algunas opciones son: Google Meet, Microsoft Teams, Jitsi Meet, Jami, Nextcloud Talk, Riot.im, BigBlueButton, Wire, Skype, Hangouts, WhatsApp, FaceTime, Google

muchas personas, e incluso, el medio para dar continuidad a asuntos laborales, la vida cotidiana y la comunicación con familiares y amigos. Lo novedoso de estos servicios para muchos usuarios y la aparición de algunas vulnerabilidades en ciertas plataformas[77], supone para los ciberdelincuentes la oportunidad para el acceso no autorizado a información, robo de credenciales y acceso a los distintos recursos del dispositivo (como micrófono, cámara, etc.).

Por lo anterior, es necesario promover la adecuada protección de los usuarios para evitar incidentes al usar estos servicios tales como:

- Informarse sobre las políticas de privacidad y las medidas de seguridad que implementa el servicio que se desea utilizar.
- Descargar e instalar la aplicación correspondiente desde la página Web oficial del desarrollador o desde las tiendas oficiales de apps.
- Mantener actualizada la aplicación que se utilice, pues es a través de este proceso que se puede asegurar que las vulnerabilidades detectadas y corregidas por el desarrollador se están implementando.
- Al organizar una videoconferencia se recomienda tener en cuenta:
  - En el caso de reuniones privadas, compartir el enlace directamente con los participantes, haciendo uso de las funciones para

Duo, Discord, Gruveo, Instagram, Snapchat, Meet, Line, Blue Jeans, Teams, Webex, Facebook Messenger, ZooRoom, Zoom, Signal, Viber, WeChat, etc.

Si bien el equipo mínimo necesario para participar en videoconferencias es un equipo Atom o Celeron con 2 GB de RAM, casi todas las plataformas de videoconferencia recomiendan un equipo de cómputo como el i3 de Intel con 2GB de RAM -o su equivalente en AMD- para ser partícipe, en el caso de ser el anfitrión de la reunión se recomienda un equipo i5 con 4 GB de RAM -o su equivalente en AMD-. En cualquier caso, es común hacer un uso intenso de CPU, generando más calor que en su uso cotidiano. Esto ocasionará que los ventiladores del equipo trabajen a toda su capacidad para disipar el calor generado. Por ello es recomendable que el equipo esté conectado a la corriente eléctrica, cerrar las aplicaciones innecesarias y que el equipo esté bien ventilado, además de no maximizar la ventana de visualización de la videoconferencia pues esto generará mayor uso de CPU.

En el caso de usar dispositivos móviles como tabletas o teléfonos inteligentes para ser partícipe en videoconferencias, es recomendable instalar las aplicaciones de videoconferencia respectiva y tratar de no hacerlo mediante el navegador, para así optimizar el uso de Hardware y batería.

[77] Una de las aplicaciones más usadas es Zoom, la cual ha tenido múltiples problemas de seguridad y privacidad.

compartir de las propias aplicaciones, y evitando el uso de redes sociales o canales de comunicación abiertos que podrían promover accesos no deseados.

- Proteger la conferencia con una contraseña robusta, para restringir el acceso a ésta a personas no autorizadas.

- Si la plataforma la incorpora, activar la funcionalidad que permite al organizador verificar y, en su caso, aprobar el acceso de los participantes que deseen acceder a la videoconferencia.

- Los participantes en videoconferencia deben evitar compartir su escritorio de forma predeterminada ya que esto podría provocar fugas de información.

- Se debe cuidar el encendido del micrófono y la cámara de vídeo para evitar situaciones incómodas o embarazosas.

- Si la videoconferencia es grabada, el organizador debe comunicarlo a los participantes.

4.13 Cómo Tomar, Enviar y Almacenar Contenido Íntimo

Cuando gran parte de nuestra comunicación ocurre en línea, sextear, video grabar, grabar audio, fotografiar o elaborar videos reales o simulados de contenido íntimo es tan saludable y natural como tener relaciones sexuales según dicen los expertos. Poder intercambiar instantáneamente dicho material con alguien sin importar la distancia puede ser muy divertido, pero la facilidad puede hacer que ignores las posibles complicaciones.

Al igual que tener relaciones sexuales, enviar contenido íntimo puede tener consecuencias no deseadas de por vida con las que quizás no estés dispuesto a lidiar[78]. Pero podemos minimizar fácilmente los riesgos y protegernos si estamos seguros.

[78] En México existe la "Ley Olimpia", está no se refiere a una ley como tal, sino a un conjunto de reformas legislativas encaminadas a reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como ciberviolencia.

Las siguientes son conductas que atentan contra la intimidad sexual:

Envío de Contenido Sexual Íntimo Repasemos lo básico. No existe contenido íntimo completamente seguro. Simplemente vamos a seguir adelante y decirlo: una vez que generemos el contenido íntimo, ya sea que presionemos el botón Enviar o no, perderemos el control total de dicho material.

Siempre existe la posibilidad de que se tenga acceso al medio con el cual generamos y/o almacenamos el contenido sexual íntimo y un tercero pueda exponer, distribuir, difundir, exhibir, reproducir, transmitir, comercializar, ofertar, intercambiar y compartir imágenes, audios o videos de contenido se-xual almacenado en nuestro dispositivo y a sabiendas de que no existe consentimiento, mediante materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico sea difundido.

La tecnología no puede arreglar a los humanos que no son de confianza, pero puede ayudarlo a expresar sus límites y hacer que sea un poco más difícil violarlos. Claro, algunas aplicaciones te notificarán cuando alguien tome una captura de pantalla de tu imagen, pero en realidad no evitarán que lo hagan. Un destinatario también puede simplemente usar otro dispositivo para tomar una foto de la pantalla sin alertarlo.

¿Usted o su pareja son menores de edad? No tome, envíe, reciba, comparta o almacene contenido sexual íntimo. No hay matices sobre esto: el contenido sexual íntimo de menores son pornografía infantil, y su producción, almacenamiento y distribución está en contra de la ley. Incluso si un intercambio de imágenes fue consensuado con entusiasmo, y usted fue quien se tomó contenido sexual íntimo, muchos países aún podrían considerarlo un delito grave solo porque es menor de edad.

- Video grabar, grabar audio, fotografiar o elaborar vídeos reales o simulados de contenido sexual íntimo, de una persona sin su consentimiento o mediante engaño.
- Exponer, distribuir, difundir, exhibir, reproducir, transmitir, comercializar, ofertar, intercambiar y compartir imágenes, audios o videos de contenido sexual íntimo de una persona, a sabiendas de que no existe consentimiento, mediante materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico.

Por su parte, se entiende como violencia digital aquellas acciones en las que se expongan, difundan o reproduzcan imágenes, audios o videos de contenido sexual íntimo de una persona sin su consentimiento, a través de medios tecnológicos y que por su naturaleza atentan contra la integridad, la dignidad y la vida privada de las mujeres causando daño psicológico, económico o sexual tanto en el ámbito privado como en el público, además de daño moral, tanto a ellas como a sus familias.

Cumplir con la Etiqueta Básica de Sext Esto puede ser evidente, pero existen reglas básicas de decencia cuando se trata de enviar contenido sexual íntimo.

- Si recibe uno, no lo comparta con nadie más, es para usted y sólo para usted. Cuando comparte contenido sexual íntimo, no solo está violando la confianza de la persona que la envió, sino que también hace que sea más probable que termine en las manos equivocadas, o peor aún, en Internet. En muchos países, compartir contenido sexual íntimo sin su consentimiento también puede ser un delito grave. Simplemente no lo hagas.
- No publiques contenido sexual íntimo de otra persona en línea.
- Como con todas las cosas sexys, el consentimiento es clave. Respétalo. No envíe contenido sexual íntimo no solicitado, especialmente a personas que no conoce. Si estás en una relación con alguien, no importa cuán casual sea, ten una conversación sobre cómo se siente acerca del contenido sexual íntimo no solicitado. Algunos pueden recibir contenido sexual íntimo en medio de su jornada laboral, mientras que otros no. Habla con tu pareja sobre sus gustos y límites, y hónralos.

En Caso de Duda, Abstenerse Envía contenido sexual íntimo sólo a aquellos que conoces y en los que confías. Esto excluye a las personas con las que has coincidido en aplicaciones de citas pero que nunca conociste, los contactos en línea que ni siquiera estás seguro de que sean reales o las personas que te dan la más mínima pista de que no son confiables.

El mayor riesgo de enviar contenido sexual íntimo es que la persona al otro lado del dispositivo es menos confiable de lo que crees. O que son dignos de confianza hoy pero lo serán menos en el futuro, después de una ruptura, por ejemplo. Saber en quién confiar está lejos de ser una ciencia perfecta, pero solo hacerte la pregunta antes de enviarles contenido sexual íntimo podría ahorrarte algunos problemas.

El perder o dar acceso al dispositivo donde almacenamos contenido sexual íntimo sin la adecuada protección, puede poner nuestro contenido sexual íntimo a disposición de terceros que no dudarán en compartir dicho material. Sí, esto suena aterrador, pero no significa dejar de generar y/o enviar contenido sexual íntimo por completo. En cambio, debemos concentrarnos en administrar las cosas que podemos controlar.

Cómo Tomar Contenido Sexual Íntimo de Forma Segura La mejor manera de mantener seguro el contenido sexual íntimo es mantenerla en el anonimato. De esa manera, incluso si su material termina en línea, será difícil identificarlo.

- Recorta o Cubre tu Cara
- Ir sin rostro es la base del anonimato. Si esto no funciona con tu visión artística, sé creativo y opta por otras formas de hacerte inidentificable. Utilice ángulos nítidos para mantener su rostro fuera del marco o envuelto en sombras, o dispare con un flash brillante en un espejo, por ejemplo.
- Si usa una máscara, asegúrese de que cubra lo suficiente de su cara.
- Oculte cualquier tatuaje, marca de nacimiento y marcas de belleza
- Use el encuadre y los ángulos de la cámara para mantener los identificadores únicos ocultos a la vista. Si una gran parte de su cuerpo está cubierta de tinta, considere usar accesorios para cubrirlo. Una vez más, la creatividad es clave: una prenda de vestir, una bufanda o una cortina pueden ser útiles.

Si necesita consejos, consulte el contenido de fotografía de Boudoir en YouTube y TikTok. Esto no solo te ayudará a perfeccionar las poses y los ángulos que mostrarán tu hermoso cuerpo, sino que también aprenderás cómo hacer que tu entorno funcione a tu favor.

Considere su Entorno Si alguien echara un vistazo dentro de tu habitación, probablemente descubriría muchas cosas sobre ti. No dejes que tu estilo único te desanime. Encuentre cualquier cosa que pueda revelar información personal sobre usted y asegúrese de que no esté en el marco. Esto incluye fotos, diplomas y notas adhesivas.

Tenga en cuenta que algo no tiene que tener sus datos personales para ser revelador. Las personas que han estado en tu casa podrían identificarla fácilmente por un cartel de una banda o una pintura en tu pared.

Al elegir un escenario para tu contenido sexual íntimo, mantenlo lo más sencillo posible. Las paredes en blanco y los azulejos del baño anodinos son fondos perfectos para tomas sexys.

Finalmente, manténgase alejado de ventanas grandes y abiertas. Los puntos de referencia conocidos podrían asomarse y ser suficientes para rastrear el contenido sexual íntimo hasta su hogar y hasta usted. Además, es posible que desee mantener a los vecinos fuera de su sesión de fotos, a menos que esté interesado en eso.

Haz Siempre Algo de Postproducción. Cuando se trata de contenido sexual íntimo, las herramientas de recorte y corrección incluidas en la mayoría de los programas de edición de vídeos y fotos son tus mejores amigos. La herramienta de recorte (un icono que parece dos ángulos rectos superpuestos) te permitirá cambiar el marco de la imagen, recortando todo lo que no quieras que aparezca. Esta podría ser tu cara o ese cesto desbordante en la esquina de tu habitación.

La herramienta de curación (un ícono que parece un vendaje) lo ayudará a desenfocar la información en el fondo, junto con pequeños tatuajes, marcas de nacimiento, marcas de belleza, imperfecciones y cualquier otra cosa que desee eliminar con el aerógrafo.

La descarga de aplicaciones como Snapseed (gratis para Android e iOS) o Photoshop Express (gratis para Android e iOS) en su teléfono o computadora lo ayudará a modificar todas las cosas que podría haber olvidado mientras tomaba la fotografía. También le proporcionarán una amplia biblioteca de filtros para que se vea aún más como un bocadillo.

Desactivar los Servicios de Ubicación Cada foto que toma tiene metadatos[79] adjuntos, incluida la cámara que usó, el sistema operativo que ejecuta su dispositivo y, lo adivinó, su ubicación en el momento en que presionó el botón del obturador. Incluso si su rostro no se muestra, alguien podría usar esos metadatos (véase sección 4.18) para confirmar su identidad a través de su ubicación o dirección.

Si está utilizando un dispositivo móvil, apague los servicios de ubicación antes de tomar la foto. En Android, deslícese hacia abajo desde la parte superior de la pantalla para abrir el menú de configuración rápida y toque el icono de ubicación para desactivar la señal de GPS. Además, abra la aplicación de su cámara y toque el icono del engranaje para acceder a su configuración. Una vez que esté allí, toque el interruptor junto a Guardar ubicación para evitar que la aplicación agregue su paradero a sus metadatos.

En iOS, vaya a Configuración, luego a Privacidad y seleccione Servicios de ubicación. Allí, busque la aplicación de la cámara y, en Permitir acceso a la ubicación, elija Nunca.

Si olvidó hacer esto, puede eliminar los metadatos de ubicación de su imagen más tarde usando macOS. Abra la foto usando Vista previa y presione el comando + I, o vaya a Herramientas y haga clic en Mostrar inspector, que le mostrará toda la información adjunta a su archivo. En la pestaña Más información (segunda a la derecha), elija la pestaña GPS (tercera a la derecha). Luego, en la parte inferior del cuadro de diálogo, haga clic en Eliminar información de ubicación. La pestaña GPS debería desaparecer.

Puedes hacer lo mismo en Windows. Haga clic derecho en uno o más

[79] Al tomar fotografías o vídeos es recomendable por seguridad desactivar el guardado de datos *Exif* (Exchangeable Image File) también conocidos como metadatos, ya que estos contienen información sobre la cámara, sobre la fotografía y sobre su origen como ubicación por GPS, la hora de creación, la última modificación, etc. En GNU/Linux podemos instalar el paquete *ExifTool* que permite conocer y borrar los datos *Exif* en fotografías. Para instalarlo usamos:

```
# apt install libimage-exiftool-perl
```

Para visualizar los datos Exif, usamos:

```
$ exiftool imagen.gif
```

Para borrar todos los datos Exif, usamos:

```
$ exiftool -all=imagen.gif
```

archivos, seleccione Propiedades y vaya a Detalles. En la parte inferior del cuadro de diálogo, haga clic en Eliminar propiedades e información personal y luego marque la casilla junto a Eliminar las siguientes propiedades de este archivo. En la parte inferior, haga clic en Seleccionar todo y luego presione Aceptar. Esto borrará todos los metadatos de los archivos seleccionados.

Desactive la Sincronización Automática con sus Servicios en la Nube Enviar fotos directamente desde el carrete de su cámara a su espacio personal en la nube es útil, pero es una responsabilidad cuando se trata de contenido sexual íntimo.

Antes de tomar su contenido sexual íntimo, asegúrese de desactivar la sincronización entre su dispositivo y todos los servicios en la nube conectados. En Android, abre la aplicación Google Photos, toca tu avatar (arriba a la derecha) y luego Copia de seguridad. Una vez allí, apague el interruptor junto a Copia de seguridad y sincronización. En iOS, desactive las fotos de iCloud yendo a Configuración, tocando su nombre, eligiendo iCloud, luego Fotos y desactivando el interruptor junto a Fotos de iCloud.

Asegúrate de eliminar tus vídeos, fotos del carrete de la cámara y de la papelera, o muévelas a una carpeta segura antes de volver a activar la sincronización.

Cómo Enviar Contenido Sexual Íntimo de Forma Segura Ahora es el momento de entregar tu contenido sexual íntimo y sacudir el mundo de tu pareja. Elige una plataforma segura: Cualquier cosa que no tenga encriptación de extremo a extremo (E2E), que protege su contenido de la intercepción en su camino hacia el destinatario y evita que la empresa propietaria de la plataforma acceda a él, está fuera de discusión. Esto significa que no hay Facebook Messenger o Instagram. Snapchat usa encriptación E2E en fotos y videos, pero no en mensajes, y aunque te permite saber cuándo alguien tomó una captura de pantalla de tu foto, no evita que lo haga.

Tu apuesta más segura es Signal. Está encriptado E2E, puede hacer que los mensajes desaparezcan un mínimo de cinco segundos después de verlos y los chats seguros evitan que los usuarios tomen capturas de pantalla. Vale la pena señalar que esto no impide que alguien tome una foto de la pantalla, pero en lo que respecta a las aplicaciones de mensajería tradicionales, Signal puede ser su mejor opción.

Si está dispuesto a gastar dinero en su privacidad, Disckreet es una apli-

cación de mensajería diseñada para compartir textos e imágenes subidas de tono. Disponible para iOS y Android, esta plataforma está encriptada E2E, protegida por un código de acceso y brinda a los usuarios control unilateral sobre su contenido. Esto significa que usted decide cuándo su pareja puede ver una foto que envió y puede eliminar la imagen de forma remota desde su teléfono. La versión gratuita de Diskreet limita el tamaño y la cantidad de archivos que puede compartir en un día, pero puede suscribirse por $ 1 al mes para compartir sin restricciones.

Obtenga Toda la Ayuda que Pueda Si está atascado usando una aplicación poco segura, asegúrese de activar todas las funciones que pueden dificultar la descarga o la captura de pantalla de sus fotos en el otro extremo. Una vez que haya terminado de sextear, no olvide pedirle explícitamente a su pareja que elimine sus fotos.

Incluso si no lo hacen, esto dejará en claro que cuando compartió esas imágenes, estaban destinadas solo para los ojos de su pareja. Si los comparten o los publican en línea, legalmente constituye una violación de su privacidad.

Ejercita Algunos Buenos Elementos Esenciales de Ciberseguridad Asegúrate de estar seguro en línea en general. Comience por proteger todas sus cuentas y dispositivos con contraseñas, patrones, PIN, códigos de acceso o datos biométricos únicos y seguros (véase sección 4.1). Si hacer un seguimiento de toda esa información es demasiado difícil para usted, descargue un administrador de contraseñas y no olvide habilitar la autenticación de dos factores en todas sus cuentas.

Ya deberías estar haciendo todo esto, pero es especialmente importante si estás intercambiando contenido sexual íntimo. Desea que sea lo más difícil posible para cualquier persona acceder a su contenido sexy al ingresar a sus cuentas o dispositivos (véase sección 4.3).

Cómo Almacenar de Forma Segura Contenido Sexual Íntimo Lo que haga después de enviar contenido sexual íntimo dependerá de si desea eliminarlo o agregarlo a su archivo personal. Si puede, elimine el contenido sexual íntimo en la plataforma que utilizó para enviarla para que ni usted ni el destinatario tengan acceso a ella. Si no desea dejar absolutamente ningún rastro, también debe eliminar el archivo en su dispositivo.

Pero tal vez hiciste contenido sexual íntimo muy bueno y no quieres que se pierda en el olvido. Aquí es cuando necesita asegurar su archivo. Los servicios de almacenamiento en la nube son susceptibles a piratería y fugas de datos, por lo que es posible que desee almacenar su contenido sexual íntimo localmente (véase sección 4.3).

La forma más fácil es mover su contenido sexual íntimo a una carpeta protegida con contraseña en su dispositivo. En Android, vaya a la aplicación Archivos y luego a Imágenes e imágenes. Seleccione su contenido sexual íntimo presionándolo prolongadamente, toque los tres puntos en la esquina superior derecha de la pantalla y elija Mover a la carpeta segura. Para acceder a esa carpeta, deberá proporcionar un patrón de seguridad, un código de acceso o una función biométrica, que puede ser la misma que usa para desbloquear su teléfono o algo completamente diferente. También puede ocultar la carpeta, de modo que si alguien entrara en su dispositivo, no podría verlo ni buscarlo.

Windows 10 y 11 tiene una característica similar que le permite usar el Explorador de archivos para proteger cualquier archivo o carpeta con una contraseña. Simplemente haga clic con el botón derecho en el elemento, vaya a Propiedades y luego a Avanzado. Haga clic en Cifrar contenido para proteger los datos en la parte inferior del cuadro de diálogo y haga clic en Aceptar y luego en Aplicar. En el siguiente cuadro de diálogo, elija si desea cifrar solo el archivo o toda la carpeta donde se encuentra, luego haga clic en Aceptar.

El sistema operativo de la computadora de Apple también le permite crear carpetas protegidas con contraseña. Guarde su contenido sexual íntimo dentro de una carpeta, abra Disc Utility y vaya a Archivo, Nueva imagen e Imagen de la carpeta... Luego, use la ventana emergente del Finder para encontrar la carpeta de su interés y haga clic en Elegir. En Cifrado, elija su protocolo, luego ingrese y verifique su contraseña. Finalmente, en Formato de imagen, elija leer/escribir y presione Guardar. También puede proteger archivos individuales en Vista previa, siempre que se guarden como archivos PDF, y use la aplicación Notas para crear archivos protegidos con fotos incrustadas.

No hay una solución integrada para iOS, pero puede descargar una aplicación gratuita de bloqueo de archivos que hará el mismo trabajo que la "carpeta segura" de Android en su iPhone.

Otra alternativa es mover su contenido sexual íntimo a un disco duro externo, que puede cifrar y almacenar en un lugar seguro (véase sección 4.3).

El Contenido Sexual Íntimo Seguros son un Esfuerzo de Equipo Nada de lo que haga para garantizar que el contenido sexual íntimo seguro sea realmente seguro si el destinatario no se molesta en configurar un código de acceso para bloquear su dispositivo.

Si su pareja no tiene conocimientos tecnológicos, tómese el tiempo para enseñarle lo que debe hacer para protegerlo a usted y a ellos mismos aplicando algunos elementos esenciales de ciberseguridad (véase sección 4.1 y 4.3).

4.14 Protección Contra Ataques con Técnicas de Inteligencia Social

Los ataques de ingeniería social buscan engañar a los usuarios para obtener nombres de usuario, contraseñas, así como otra información sensible o bien que el usuario descargue archivos y/o instale programas que vulneran la seguridad del equipo de cómputo. La capacidad de identificar un ataque de ingeniería social minimiza en gran medida, el riesgo de ser víctimas de los ciberdelincuentes y ver comprometida información personal o de la organización para la que trabajamos. Para ello, se recomienda:

- Estar alertas ante comunicaciones, como llamadas, correos electrónicos, mensajes cortos (SMS), enlaces de teleconferencias e invitaciones de calendario de remitentes desconocidos.
- Antes de abrir cualquier enlace, archivo anexo, mensaje de texto o llamada de un remitente desconocido, hay que preguntarse lo siguiente:

  ◦ ¿Espero esa información? Si el mensaje proviene de un remitente desconocido (persona u organización), analizar bien antes de responder o hacer clic y/o descargar cualquier archivo adjunto.

  ◦ ¿Reconozco al remitente? Comprobar si la dirección está bien escrita (verificar que no haga falta ninguna letra, por ejemplo) y si el dominio (la terminación del correo electrónico) es de confianza y corresponde al nombre de quien envía el mensaje.

  ◦ ¿Solicitan que haga algo? Los correos electrónicos fraudulentos (Phishing) o los mensajes de texto de este tipo (Smishing) suelen pedir que se realice alguna acción como: hacer Clic en un hipervínculo, descargar algún archivo, responder al mensaje proporcionando información personal, etc. Con frecuencia, buscan generar

una sensación de urgencia y provocar una reacción inmediata e irracional. Es necesario analizar con calma antes de proporcionar cualquier información que pudiera resultar comprometedora.

- Se debe desconfiar, particularmente, de los mensajes que parecerían genéricos (como "Estimados:", "A quien corresponda:", etc.).

- En el caso de comunicaciones referentes a instituciones bancarias y financieras, se recomienda nunca dar clic en los enlaces contenidos en un correo o mensaje y no proporcionar información de acceso a tus cuentas. Si tienes alguna duda, debes contactar directamente a tu institución financiera (utilizando el número telefónico que viene atrás de tu tarjeta, por ejemplo) para más orientación.

Siempre hemos de tener presente que garantizar la protección absoluta de su información digital es difícil sino imposible, pero debemos aprovechar todas las herramientas y avances que están a nuestro alcance. De esta forma, estaremos mejorando la seguridad de nuestros datos personales y sus contenidos. Son pequeños gestos diarios que, en caso de problemas, marcarán una gran diferencia.

Usuarios Subestiman el Poder de la IA para Generar Fraudes
La mayoría de los usuarios desconocen que la Inteligencia Artificial puede generar fraudes como Deepfakes. La Inteligencia Artificial ya forma parte de nuestras vidas, aunque quizá no lo notemos, sistemas como ChatGPT están transformando diversas tareas. Pero al parecer los usuarios no son conscientes de que hay riesgos y subestiman la capacidad de esta tecnología para cometer fraudes.

La mayoría de las personas creen que son capaces de identificar las posibles estafas en línea, por ejemplo, distinguir entre un vídeo falso o Deepfake, y uno real. Pero es más difícil de lo que la mayoría considera y con el tiempo será peor.

De acuerdo con un estudio de Jumio en 2023, proveedor de soluciones automatizadas e integrales de verificación de identidad, la mayoría de los consumidores desconoce que es la IA generativa y las tecnologías Deepfake. El riesgo de ello es que esas tecnologías podrían acelerar el fraude de identidad

haciendo cada vez más importante contar con sistemas para la verificación y autenticación en línea.

El estudio también destaca que los consumidores parecen sobreestimar su capacidad para detectar Deepfakes, lo que puede hacerlos aún más vulnerables a los ataques. En la encuesta participaron 8,055 consumidores adultos de Reino Unido, Estados Unidos, Singapur y México.

Según los resultados, más de dos tercios (67%) afirman conocer las herramientas de IA generativa, como ChatGPT, DALL-E y Lensa AI, que pueden producir contenidos inventados, incluidos vídeos, imágenes y audio. Los consumidores de Singapur son los que más las conocen (87%) y los del Reino Unido los que menos (56%).

También mencionan que el 52% de los encuestados cree que podría detectar un vídeo Deepfake. Lo que demuestra un exceso de confianza por parte de los consumidores.

Lo anterior a pesar de que los datos de Jumio demuestran un aumento constante en el uso de Deepfakes cada vez más sofisticados en todo el mundo y en todos los sectores, con una mayor presencia en las industrias de de pagos y criptomonedas.

¿Cómo Estamos en México? Cifras recientes de la Asociación de Internet de México muestran que 7 de cada 10 usuarios digitales en el país fueron víctimas de algún tipo de fraude cibernético en 2022. Además, 1 de cada 3 víctimas había sufrido suplantación de identidad.

Y es que, como menciona Jumio, el conocimiento superficial da paso al uso potencialmente perjudicial. A pesar de lo anterior cada vez más consumidores van comprendiendo cómo estas tecnologías podrían utilizarse para alimentar la usurpación de identidad. De hecho, más de la mitad (57%) cree que el robo de identidad en línea será más fácil como consecuencia de ello.

No obstante Philipp Pointner, director de identidad digital de Jumio, advierte que conocer los riesgos no será suficiente: "incluso la mejor educación nunca podrá detener por completo el uso de tecnologías emergentes por parte de un estafador. Las organizaciones en línea deben tratar de implantar sistemas de verificación biométrica multimodal que puedan detectar los Deepfakes y prevenir el uso de información personal robada".

Con base en los resultados se sabe que más de dos tercios (68%) de los consumidores están dispuestos a utilizar una identidad digital para verificarse en línea. Los principales sectores en los que preferirían una identidad digital a

un documento de identidad físico (como la licencia de conducir o el pasaporte) son los servicios financieros (43%), la administración pública (38%) y los servicios de salud (35%).

Risgos al Usar ChatGPT para Trabajar Usar internet siempre implica cierto riesgo, ya sea en el ámbito personal como en el profesional. Pero después de ver todo lo que pueden hacer inteligencias artificiales como ChatGPT, implementarla en las rutinas de algunos trabajos parece inevitable (de hecho, en algunas profesiones puede hasta marcar la diferencia). El problema está en que algunas empresas como Samsung y Apple están prohibiendo su uso por cuestiones de confidencialidad. Si empleas ChatGPT para tu trabajo, merece la pena conocer a fondo su funcionamiento, riesgos y las condiciones que aceptas cuando la usas.

ChatGPT y otros modelos generativos con inteligencia artificial se han vendido como la herramienta definitiva de productividad, la panacea para escribir artículos por ti, correos electrónicos, tus redes sociales, resúmenes de largos y complejos textos y un largo etc. Estos meses hemos tenido la oportunidad de verlo y comprobarlo nosotros mismos.

El vicepresidente de investigación de privacidad de Gartner Nader Henein da una imagen muy acertada de lo que es en realidad ChatGPT para Mashable: es una especie de extraño afable sentado delante de ti en el autobús grabándote con la cámara del móvil. En ese escenario, ¿nos imaginamos compartiendo información sensible? El sentido común dice que no.

Pero la tentación de reducir trabajo rutinario está ahí, llamándote, lo que nos lleva a pensar en estos Chatbots en algo parecido a una calculadora o una hoja de cálculo cuando en realidad esa información va a la nube, es analizada y se queda allí "para siempre". El caso Samsung fue uno de los primeros y más sonados: emplearon ChatGPT para verificar su código y así, sin darse cuenta, revelaron datos comerciales.

Porque ves que el Chatbot de OpenAI tiene una interfaz sencilla e intuitiva, un lenguaje que parece humano, un sentido del humor que te puede sacar una sonrisa y un vasto fondo de armario para resolver dudas, corregir errores, darte ideas ... cualquier día, a cualquier hora del día (aunque si usas la versión gratis, a veces puedes encontrártela saturada). Y así es fácil relajarse y tratar de exprimirla al máximo.

Recientemente ChatGPT implementó una función que mejora la privacidad de quienes usan su modelo: la posibilidad de evitar que almacene nues-

tros Chats para usarlos posteriormente para el entrenamiento, una de las medidas que han aflojado la soga al cuello de OpenAI en Europa, donde llegó a estar prohibido en Italia. Es un paso adelante, pero todavía quedan riesgos en el camino.

Sirva como ejemplo las declaraciones de Sam Altman, el CEO de OpenAI, en su perfil de Twitter, donde ha reconocido abiertamente los riesgos de confiar en ChatGPT: "es un error confiar en él para cosas importantes en este momento, tenemos mucho trabajo por hacer en fiabilidad y robustez."

¿Qué riesgos implica usar ChaGPT? Para profundizar en los riesgos implícitos de ChatGPT vamos a repasar primero lo que dice la propia OpenAI sobre su uso, después sobre el modelo en cuestión y finalmente sobre la plataforma.

Chats almacenados en servidores. Como detallan las FAQ de ChatGPT, el contenido se almacena en sus sistemas y otros "sistemas de servicios confiables en Estados Unidos y otras partes del mundo". Pero aunque OpenAI en general elimina la información personal identificable, antes estos datos en crudo están en sus servidores y parte de su personal tiene acceso a ellos para tareas como afinar sus modelos, proporcionar soporte, detectar abuso y cumplir con las obligaciones legales.

Los Chats se usan para entrenar al modelo (aunque puedes deshabilitarlo). Salvo que digas lo contrario, OpenAI explica que usar los datos proporcionados por usuarios y usuarias para mejorar sus modelos. Sobre el anonimato de los datos, OpenAI detalla que puede "agregar o anular la identificación de la información personal y usar la información agregada para analizar la efectividad de nuestros servicios". En la práctica, esto posibilitaría que pudiera filtrar secretos comerciales ofreciendo el "qué" y el "quién". Aunque antes la opción de dejar de compartir datos para el entrenamiento pasaba por enviar un formulario de Google cumplimentado, ahora dispone de una opción en su configuración para desactivarlo antes. Eso sí, incluso en el modo incógnito, las conversaciones se guardan en sus servidores durante 30 días.

Tus datos no se comercializan a terceros. Según OpenAI, no se comparten datos de los usuarios a terceros con fines de marketing o publicidad. Pero ojo, porque sí que comparte datos con vendedores y proveedores de servicios para el mantenimiento y operación de la Web.

Posibles brechas de seguridad y ataques. Aunque todo lo anterior jugase en tu favor, siempre está el factor externo: que alguien ajeno a OpenAI

quebrase el acceso y robase sus datos, un riesgo inherente al propio funcionamiento del sistema mediante servidores. Y de hecho, ya ha pasado: una brecha de seguridad propició que vieran la luz datos personales de sus usuarios, entre ellos, el primer mensaje de nuevos Chats e información de pago de quienes usan ChatGPT Plus.

La fiabilidad de sus datos. Lo advertía Altman y lo hemos visto: con código erróneo que provocó la prohibición de su uso en Substack o del abogado que se ha visto en problemas legales por usar referencias proporcionadas por ChatGPT que no existían. La inteligencia artificial puede agilizar tareas y orientarte, pero por el momento no debe ser la referencia absoluta y sí una orientación. Máxime cuando como en ChatGPT, no proporciona la fuente para validar los datos.

Así que si tu idea es usar ChatGPT en el trabajo para que te explique cosas que no entiendes, escribir informes o analizar datos ... y no existe una normativa específica corporativa, entonces procede con precaución. ChatGPT ya advierte sobre el uso de información personal, pero la profesional confidencial también puede salir de control.

4.15 Protección de Dispositivos Personales en Redes Corporativas

El creciente uso de dispositivos móviles personales (computadoras portátiles, tabletas y teléfonos inteligentes) ha necesitado especial atención al momento de su uso en redes corporativas -inclusive se ha acuñado el término BYOD (Bring Your Own Device) esto ha cobrado especial importancia en épocas de confinamiento- desde casa, la propia oficina o cualquier otro lugar, aceptando su uso compartido, tanto para las tareas profesionales de uso corporativo como para las personales de los empleados.

Una buena parte de los riesgos que conlleva el BYOD estriba en el uso que se haga de los dispositivos el usuario. Para minimizar los riesgos derivados del uso de dispositivos BYOD a la hora de integrarlos dentro de las organizaciones y obtener el mayor rendimiento posible de los mismos, se sugiere los siguientes consejos:

- Involucrar a los usuarios en la protección de sus propios dispositivos, los administradores de TIC deben incentivar, concientizar y formar al

usuario para que tome medidas destinadas a proteger los datos corporativos y personales.

- Los administradores de TIC deberán mantener una base de datos de usuarios y dispositivos y a que recursos de la empresa acceden, los usuarios que los manejan y los privilegios de seguridad que les permitan autentificar y autorizar estos usuarios y dispositivos.

- Se deben tomar precauciones con el almacenamiento de datos del trabajo, instalando herramientas que salvaguarden los datos corporativos, especialmente a la hora de utilizar aplicaciones de intercambio de archivos en la nube. A la hora de trabajar con los datos de la empresa, es más seguro tener estos almacenados en la nube y consultarlos, que realizar un intercambio de archivos real.

- Implementar medidas de acceso seguro a la información como el cifrado de la información y la correcta autentificación de usuarios, uso de escritorios remotos o virtuales, además del uso de sistemas de redes virtuales privadas (VPN).

En cualquier caso, siempre debemos ser conscientes que los dispositivos móviles personales son más susceptibles a ser perdidos, robados o que otras personas ajenas a la empresa tengan acceso a los dispositivos y la información a la que el empleado tiene acceso. Por ello todas las medidas de seguridad que se implementen repercutirán en la seguridad general de la empresa, tomando en cuenta que el acceso a la información mediante el BYOD será siempre el eslabón más débil de toda la cadena de ciberseguridad implementada por la empresa.

4.16 Uso de Escritorios Remotos y Virtuales

Con el propósito de que cualquier usuario que cuente con un dispositivo de cómputo[80] con red[81] puedan usar, configurar o instalar aplicaciones en los ambientes computacionales que se tienen instalados en otros equipos de

[80] Puede ser computadora personal , tableta, teléfono inteligente, Chromebook corriendo algún sistema operativo como Windows, Linux, MacOS, Android, Raspberry PI, IOS, Chrome, Solaris, HP-UX, AIX, etc.

[81] ¡Claro desde casa!, sin dirección IP pública fija homologada.

cómputo de forma remota, se crearon los escritorios remotos y escritorios virtuales.

Los escritorios remotos y virtuales permiten visualizar la salida gráfica -de un sistema operativo en múltiples equipos o diversos sistemas operativos en un mismo equipo- por medio de internet (aún si la velocidad de conexión es baja). Los casos de uso son muchos y se centran muy especialmente en los ámbitos de la asistencia remota[82] y del trabajo de forma remota (teletrabajo).

Escritorio Remoto Esta es una de las muchas aplicaciones que permiten acceder a un equipo de cómputo remoto mediante internet y controlarlo como si estuviéramos delante de él -más o menos-. Con estas aplicaciones, nos ahorramos tener que desplazarnos hasta donde está el equipo de cómputo al que queremos conectarnos, y así podemos por ejemplo ofrecer asistencia remota desde nuestro equipo de cómputo o usar los programas que se tienen instalados en un equipo remoto.

Algunas opciones de escritorios remotos[83] son:

- Chrome Escritorio Remoto (de descarga y uso gratuito), donde instalamos el servidor de escritorio remoto a través del navegador Chrome (o Chromium) en el equipo de cómputo a controlar y mediante el navegador Chrome en el otro equipo, se puede acceder remotamente cuando se necesita desde cualquier lugar con internet.

- "Asistencia rápida" (o Quick Assist) de Windows 10 es una utilidad del sistema operativo que permite a dos personas compartir un equipo mediante conexión remota, pero sin necesidad de descargar ni instalar nada adicional.

Escritorio Virtual Es el acceso a un equipo de cómputo virtual en la nube, cuyo poder de procesamiento no se encuentra en un equipo de cómputo físico, sino en servidores ubicados en un centro de datos.

[82] Si algo no le funciona a alguien, estos servicios remotos nos permiten "meternos" en su equipo de cómputo y solucionarlo, incluso explicando mientras se está haciendo, porque se toma el control del teclado, ratón y pantalla, pero el usuario sigue teniendo control si quiere retomarlo y puede ver todo lo que hacemos en el escritorio remoto.

[83] Otras opciones son: Apple Remote Desktop, TeamViewer, SupRemo, Ammyy Admin, Iperius Remote, AnyDesk, VNC Connect, etc.

El usuario inicia sesión con sus credenciales y accede a un escritorio con las aplicaciones y programas instalados como si estuviera sentado frente a ese equipo de cómputo virtual.

¿Cuáles son las ventajas? los escritorios virtuales[84] tienen muchas ventajas para las organizaciones que necesitan entregar acceso a un equipo de cómputo con un conjunto establecido de aplicaciones. Se reducen los costos administrativos y mantenimiento de licencias. También facilita la solución de problemas de usuario y reduce problemas de seguridad.

Otras ventajas de esta tecnología:

1.- Administración centralizada de aplicaciones

2.- Se puede acceder desde dispositivos móviles, como teléfonos o tabletas.

3.- Facilita la aplicación de políticas organizacionales.

4.- Acelera la habilitación de nuevos puntos de trabajo.

Desde hace años existen ejemplos de estas tecnologías: "Windows Virtual Desktop" el escritorio virtual de Windows 10 sobre Microsoft Azure y recientemente con: "Cloud PC" para ofrecer "Desktop as a Service" de la división "Cloud Managed Desktops" de Microsoft.

4.17 Máquinas Virtuales

Entendamos por una máquina virtual a un programa de cómputo que simula a una computadora, en la cual se puede instalar y usar otros sistemas operativos de forma simultánea como si fuese una computadora real sobre nuestro sistema operativo huésped[85].

Una característica esencial de las máquinas virtuales[86] es que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados

[84] Ejemplo de estos productos son: VMware Horizon, Citrix Virtual Apps and Desktops, Oracle Secure Global Desktop, HP Workspace, Amazon WorkSpaces, Parrallels Remote Application Server, Microsoft Windows Virtual Desktop, etc.

[85] Tal y como puede verse reflejado en la definición de máquina virtual, en este texto nos estamos focalizando en las máquinas virtuales de sistema. Existen otro tipo de máquinas virtuales, como por ejemplo las máquinas virtuales de proceso o los emuladores.

[86] Una máquina virtual dispone de todos los elementos de un equipo de cómputo real, de disco duro, memoria RAM, unidad de CD o DVD, tarjeta de red, tarjeta de vídeo, etc., pero a diferencia de un equipo de cómputo real estos elementos en vez de ser físicos son virtuales. Así, una vez instalado un sistema operativo en la máquina virtual, podemos usar el sistema operativo virtualizado del mismo modo que lo usaríamos si lo hubiéramos instalado en nuestro equipo de cómputo.

por ellas. Estos procesos no pueden escaparse de esta "computadora virtual". Uno de los usos más extendidos de las máquinas virtuales es ejecutar sistemas operativos nuevos u obsoletos adicionales a nuestro sistema habitual.

De esta forma podemos ejecutar uno o más sistemas operativos -Linux, Mac OS, Windows- desde nuestro sistema operativo habitual sin necesidad de instalarlo directamente en nuestra computadora y sin la preocupación de que se desconfigure el sistema operativo huésped o a las vulnerabilidades del sistema virtualizado, ya que podemos aislarlo para evitar que se dañe.

Las máquinas virtuales son una verdadera opción para coexistir simultáneamente diferentes versiones de sistemas operativos y en un mismo sistema máquinas virtuales ejecutando las diversas versiones de un mismo programa de cómputo, además se pueden configurar para que al momento de iniciarlas siempre se ejecuten a partir de una configuración e instalación base, de tal forma que al ser lanzadas, el usuario pueda instalar, configurar e inclusive dañar la máquina virtual, pero al reiniciarse la máquina virtual en una nueva sesión, se regresa a la configuración de la versión base, de esta forma no hay posibilidad de infección de virus entre diversos lanzamientos de sesiones de la máquina virtual.

El uso de las máquinas virtuales es variado, flexible y permite ser usado en diversos ámbitos de la educación, del desarrollo y prueba de programas de cómputo y en general, en Ciencias e Ingeniería. Algunas de las utilidades y beneficios que podemos sacar de una máquina virtual son los siguientes:

- Para aprender a instalar, probar diversas opciones de configuración y usar múltiples sistemas operativos. El proceso de instalación de la máquina virtual no requiere crear particiones adicionales en nuestro disco ni alterar la configuración de la máquina anfitriona.

- Para usar un Software que no está disponible en nuestro sistema operativo habitual. Por ejemplo, si somos usuarios de Linux y queremos usar Photoshop, lo podemos hacer a través de una máquina virtual.

- En ocasiones tenemos que usar Software que únicamente se puede ejecutar en sistemas operativos obsoletos -Windows XP por ejemplo-, podemos crear una máquina virtual con dicho sistema y usar el Software de forma aislada sin preocuparnos de sus vulnerabilidades.

Algunas opciones de manejadores de máquinas virtuales son: Virtualbox, Vmware Workstation Player, Parallels, Windows Virtual PC, QEMU/KVM.

- Podemos experimentar en el sistema operativo que corre dentro de la máquina virtual haciendo cosas que no nos atreveríamos a realizar con nuestro sistema operativo habitual, como por ejemplo, instalar Software no seguro que consideramos sospechoso, etc.
- Si se hace el adecuado aislamiento de una máquina virtual en la que se instale alguna versión de Windows, esta puede ser inmune a los virus y no requiere el uso de antivirus.
- Si eres un desarrollador de Software puedes revisar si el programa que estás desarrollando funciona correctamente en varios sistemas operativos y/o navegadores de Web.
- Podemos usar las máquinas virtuales para hacer SandBox[87] con el fin de ejecutar aplicaciones maliciosas o abrir correos sospechosos en un ambiente controlado y seguro.
- Para probar versiones Alfa, Beta y Release Candidate de ciertos programas y sistemas operativos.
- Para probar multitud de programas en Windows y evitar que se ensucie el registro mediante las instalaciones y desinstalaciones de los programas.
- Podemos navegar en sitios Web maliciosos sin poner en peligro nuestro equipo, ya que podemos configurar la máquina virtual para que se pierdan los cambios al ser reiniciada.

4.18 Protegiendo Nuestros Metadatos

¿Qué son los metadatos? los metadatos son "datos sobre datos" o "información sobre información" que se incluyen en archivos informáticos, normalmente de forma automática. Los metadatos se utilizan para describir, identificar, categorizar y ordenar archivos. Sin embargo, los metadatos también se pueden utilizar para desanonimizar a los usuarios y exponer información privada.

Ejemplos de metadatos incluyen:

[87] Un sistema de aislamiento de procesos o entorno aislado, a menudo usando como medida de seguridad para ejecutar programas con seguridad y de manera separada del sistema anfitrión.

- En archivos de imagen y vídeo:

  El lugar donde se tomó la foto o vídeo.

  La fecha y hora en que se tomó la foto o vídeo.

  El modelo y número de serie de la cámara utilizada.

- En archivos de documentos de texto:

  El autor del documento.

  Cambios en el documento.

Algunos tipos de archivos que guardan metadatos que pueden poner en peligro el anonimato de los usuarios:

- Audio Interchange File Format (.aiff)
- Audio Video Interleave (.avi)
- Electronic Publication (.epub)
- Free Lossless Audio Codec (.flac)
- Graphics Interchange Format (.gif)
- High Efficiency Image Format (.heic, .heif)
- Hypertext Markup Language (.html, .xhtml)
- Portable Network Graphics (PNG)
- JPEG (.jpeg, .jpg, ...)
- MPEG Audio (.mp3, .mp2, .mp1, .mpa)
- MPEG-4 (.mp4)
- Office Openxml (.docx, .pptx, .xlsx, ...)
- Ogg Vorbis (.ogg)
- Open Document (.odt, .odx, .ods, ...)

- Portable Document Fileformat (.pdf)
- Portable Pixmap Format (.ppm)
- Scalable Vector Graphics (.svg)
- Tape ARchive (.tar, .tar.bz2, .tar.gz, .tar.zx)
- Torrent (.torrent)
- Waveform Audio (.wav)
- Windows Media Video (.wmv)
- ZIP (.zip)

Es imposible encontrar y eliminar de manera confiable todos los metadatos en formatos de archivos complejos. Por ejemplo, los documentos de Microsoft Office pueden contener imágenes incrustadas, audio y otros archivos que contienen sus propios metadatos que no se pueden eliminar. Por ello se debe eliminar los metadatos de cualquier archivo antes de incrustarlo en otro documento.

Además, siempre que sea posible, debes guardar los archivos en formatos más simples. Por ejemplo, en lugar de guardar un documento de texto como un archivo .docx, puede guardarlo como un archivo .txt simple.

Metadata Anonymisation toolkit v2 permite eliminar metadatos de archivos antes de publicarlos o compartirlos, funciona en muchos formatos de archivos, incluidos:

- Archivos de imagen, como .jpeg, .png y .gif
- Archivos de LibreOffice, como .odt y .ods
- Documentos de Microsoft Office, como .docx, .xlsx y .pptx
- Archivos de audio, como .mp3, .flac y .ogg
- Archivos de vídeo, como .mp4 y .avi
- Archivar archivos, como .zip y .tar

En GNU/Linux podemos instalar el paquete mat2, mediante:

```
# apt install mat2
```

Para conocer la lista de archivos soportados usamos:

```
$ mat2 -l
```

Para visualizar los metadatos del archivo usamos:

```
$ mat2 -s nombreArchivo
```

Para remover los metadatos del archivo usamos:

```
$ mat2 -V nombreArchivo
```

en la hipótesis de eliminación de metadatos, debes tener en cuenta que mat2 no elimina el archivo en el que interviene porque deja el archivo original como está, sino que crea otro archivo.

Exchangeable Image File al tomar fotografías o vídeos es recomendable por seguridad desactivar el guardado de datos Exif (Exchangeable Image File) también conocidos como metadatos, ya que estos contienen información sobre la cámara, sobre la fotografía y sobre su origen como ubicación por GPS, la hora de creación, la última modificación, etc.

En GNU/Linux podemos instalar el paquete ExifTool que permite conocer y borrar los datos Exif en fotografías. Para instalarlo usamos:

```
# apt install libimage-exiftool-perl
```

Para visualizar los datos Exif, usamos:

```
$ exiftool imagen.gif
```

Para borrar todos los datos Exif, usamos:

```
$ exiftool -all=imagen.gif
```

4.19 Averiguar Todo Sobre Cualquier Persona en Internet

A veces no somos conscientes de que nuestro paso por internet va dejando un rastro que se puede analizar. Si estudiamos con detenimiento la información pública, en ocasiones podemos obtener una información valiosa. Una simple dirección IP pública nos puede ofrecer una gran cantidad de información del usuario. De esta forma, con relativa exactitud obtenemos dónde se encuentra geográficamente, cuál es su proveedor de servicios de Internet y más. No obstante, la recopilación de información ha ido cambiando y han aparecido nuevas técnicas y herramientas como OSINT.

Lo primero que vamos a hacer es explicar qué es OSINT. Luego explicaremos como mediante el uso herramientas como SpiderFoot HX podemos averiguar mucha información sobre una persona en concreto.

¿Qué es OSINT y qué nos Puede Aportar su Utilización? OSINT viene de las siglas en inglés Open Source Intelligence que traducido significa Inteligencia de origen abierto. En este caso nos referimos a un conjunto de técnicas y herramientas que vamos a utilizar para recopilar información pública, analizar datos y luego los correlacionamos para convertirlos en un conocimiento muy provechoso. OSINT es un conjunto de técnicas que se usan como una herramienta muy versátil y que puede utilizarse en ámbitos de Marketing, financieros, policiales y más. Además, si pensamos utilizarla para entornos relacionados con la seguridad informática nos puede ser útil para:

- Para realizar la fase de reconocimiento en pruebas de penetración o Pentesting. Así, podemos averiguar los Hosts de una organización, sacar información del Whois y más.
- La aplicación de técnicas de ingeniería social para buscar información de un usuario en redes sociales y documentos.
- Prevención de ataques informáticos en la que podemos obtener información sobre una amenaza o el potencial ciberataque que pueda recibir nuestra empresa.

En definitiva, gracias a la utilización de OSINT podemos averiguarlo todo sobre un usuario o una organización.

¿Qué es y qué nos Ofrece SpiderFoot? SpiderFoot podemos definirlo como una herramienta de reconocimiento que consulta automáticamente más de 100 fuentes de datos públicas OSINT. Su objetivo es recopilar información sobre direcciones IP, nombres de dominio, correos electrónicos, nombres y más. Su forma de funcionamiento es sencilla, especificamos un objetivo, escogemos los módulos que vamos a utilizar y continuación, SpiderFoot recopilará los datos y verá cómo se relacionan entre sí.

También tenemos SpiderFoot HX que se basa en la base del módulo de la versión de código abierto para ofrecer una funcionalidad mejorada. Esta versión es de pago y está destinada para los profesionales que desean automatizar OSINT, la inteligencia de amenazas, el descubrimiento de activos o para evaluaciones de seguridad. Entre sus características principales tenemos:

- No necesita instalación ya que está alojado y gestionado en la nube. Simplemente con registrarse ya estaremos listos para utilizarlo.
- Investigación de forma individual utilizando un sólo módulo o realizando el escaneo de múltiples objetivos de manera rápida.
- Monitoreo OSINT en el que podremos ejecutar escaneos automáticamente diariamente, semanalmente, mensualmente o programarlos a nuestro gusto.
- Notificaciones por correo electrónico y Slack cuando se produzcan cambios o finalice el análisis.
- Integración con TOR que nos proporciona que ninguna entidad escaneada sepa que somos nosotros quienes realizamos el escaneo.
- La autenticación de dos factores (2FA) significa que la seguridad de nuestra plataforma e investigaciones OSINT están seguras.
- Perfiles de escaneo personalizados.

En cuanto a esta herramienta, tiene una versión gratuita y otras de pago. La versión gratuita para conocer todo sobre un usuario, en este caso nos permite 3 escaneos por mes, el límite de duración del análisis es de 1 hora y tenemos 1 objetivo por escaneo.

Por qué Proteger tu Privacidad y qué Información Tuya se Puede Encontrar con una Búsqueda en Internet La privacidad de las personas es un derecho. Un derecho que con internet y el tratamiento de datos que hacen ya todos los negocios y servicios no es fácil proteger. O aceptas los términos y condiciones de los servicios en los que quieres crear una cuenta o no permiten crearla, algunos servicios permiten cambiar algunas opciones para no recibir comunicaciones comerciales por correo electrónico pero el tratamiento de datos está implícito en la aceptación de las condiciones.

Un buscador como Google permite encontrar datos de una persona relacionada con ella incluso pasado algún lustro. A través de las redes sociales es posible conocer cualquier cosa que una persona comparta de forma pública.

Por qué Proteger tu Privacidad internet ofrece muchas posibilidades pero también tiene otros inconvenientes. Uno de ellos es que es muy fácil perder el control de la privacidad. Una vez algo se ha publicado a través de internet es difícil revocar la información y ejercer el derecho al olvido para que esa información que se desea eliminar lo sea. Una vez publicado algo en internet cualquier persona que tenga acceso lo puede copiar o republicar en cualquier otra ubicación en la que ya no se tiene el control. Lo que en un momento se considera como poco importante publicar más adelante puede desearse que no hubiese sido publicado, el problema es que publicar algo es muy fácil pero eliminar algo publicado es muy difícil.

Las redes sociales como Facebook, Instagram o Twitter permiten relacionarse con personas en cualquier parte del mundo, conocidas y desconocidas. En estas redes sociales se publica gran cantidad de información personal que alguien interesado en conocerla le permite un acceso sencillo. Con algo tan simple como publicar el nombre y apellidos de una persona ya es posible encontrar mucha otra información utilizando un buscador como Google, cualquier página pública a la que Google tenga acceso la indexa en su buscador, y a partir de aquí a más información en las redes sociales que esté como pública.

En los términos y condiciones que nadie lee al crear una cuenta en un servicio se detallan las autorizaciones que se otorga a la empresa por el hecho de usar su servicio, en esos términos con una jerga legal difícil de entender y larga para agotar en su lectura se incluyen apartados que suele detallar que el propietario del servicio procesa y compartirá los datos con terceras partes. A partir de compartir estos datos luego uno no sabe porque le llegan

llamadas comerciales telefónicas cuando no se ha tenido relación ninguna con esa empresa de la que nos llama el comercial o mensajes SMS al teléfono móvil.

Algunos ataques informáticos son realizados de forma masiva pero otros son llevados a cabo de forma individualizada más laboriosa pero menos, que alguien que está intentando perpetrar un ataque informático sepa cosas de la víctima le da mayor conocimiento para realizar un ataque de ingeniería social.

Busca Información Tuya a Través de Datos que te Identifican es fácil averiguar cuánta información personal de uno mismo hay publicada en internet con una simple búsqueda en Google cualquier dato personal que identifique a una persona. A partir de uno de estos datos personales es posible encontrar mucha información de lo que hace una persona, que piensa a través de lo que dice, fotos suyas, de sus familiares y amigos, su ciudad y lugar de residencia, de vacaciones, lugar de trabajo y profesión, aficiones, ...

Los datos personales a través de los que averiguar la información que haya en internet de una persona son: nombre y un apellido, nombre y dos apellidos, número de teléfono móvil, dirección de correo electrónico o si utiliza su seudónimo. Si se sabe algo de esa persona como su ciudad de residencia permite descartar coincidencias en caso de obtener varias.

Pon en Google tu nombre y apellidos, tu correo electrónico, tu número de teléfono móvil que son algunas cosas que te identifican y mira la información que encuentras de ti mismo. Cuando se dice que Google conoce más de ti que tú mismo es cierto en el aspecto de que muy posiblemente hay cosas que tu ya has olvidado pero Google es capaz de encontrar.

Y Google también es capaz de reconocer texto en las imágenes. Busca también en Google Imágenes ahí también se encuentran fotos a partir de los datos identificativos.

Quizá te asustes de lo que puede conocer alguien de ti con interés por información que tú mismo has publicado. En el momento de publicar la información quizá no se le da importancia pero en el futuro en alguna circunstancia quizá se desease eliminar esa información cosa que era muy difícil o quizá no sea posible.

Cada uno es libre de hacer con su privacidad lo que mejor le parezca. Nosotros recomendamos protegerla porque es fácil perderla pero muy difícil recuperarla. La privacidad no involucra solo la de uno mismo sino también

la de los demás, si tú no le das importancia a tu privacidad otras personas si se la damos por ello si publicas datos o fotos no publiques ninguna que incluya a ninguna persona de la que no tengas su consentimiento.

La razón de utilizar un pseudónimo en internet es para utilizar un nombre que no sea el nombre y apellidos reales, esto permite separar en parte el alter ego de la persona real y desecharlo en caso de desearlo.

4.20 Prácticas de Ciberseguridad para Viajeros

Los avances tecnológicos han revolucionado nuestra forma de viajar, ofreciéndonos comodidad y conectividad al alcance de la mano. Sin embargo, estas mejoras tecnológicas también han hecho que los viajeros sean cada vez más vulnerables a las ciberamenazas.

Es crucial dar prioridad a las prácticas de seguridad, tanto dentro como fuera del hogar u oficina. He aquí algunas estrategias clave para garantizar la seguridad de los dispositivos y los datos, independientemente de su ubicación:

- Todos los dispositivos móviles y tarjetas de respaldo extraíbles deben ser cifrados (véase sección 4.3)y se debe usar una contraseña robusta para el acceso al mismo (véase sección 4.1), es decir, utilizar una combinación compleja -de al menos 15 caracteres- de letras mayúsculas, minúsculas, números y símbolos es siempre la mejor opción. Además, es imprescindible no confiarla a sus amistades y cambiarla siempre que tengan dudas de su fiabilidad.

- Actualizar regularmente los dispositivos con los últimos parches de seguridad y Firmware es crucial para protegerse de las vulnerabilidades conocidas (véase sección 4.2). Los proveedores publican constantemente estas actualizaciones para corregir errores y lagunas de seguridad y mantener a los usuarios a salvo de las ciberamenazas. Es importante mantenerse alerta y asegurarse de que todos los dispositivos estén siempre actualizados. Active las actualizaciones automáticas siempre que sea posible para asegurarse de que los parches de seguridad críticos se instalan rápidamente.

- Cuando se viaje se pueden tener la tentación de publicar sus experiencias en línea con amigos y familiares (véase sección 4.11). Sin embargo, hay que tener cuidado al revelar públicamente información sensible. Recuerde a todos sus compañeros de viaje que eviten compartir

itinerarios, detalles del hotel o información de contacto personal en las redes sociales u otras plataformas. Se desaconseja publicar fotos de tarjetas de embarque o boletos de viaje -esa información puede atraer la atención no deseada de piratas informáticos, estafadores o incluso ladrones-. Es necesario limitar la audiencia a personas de confianza y reitera la importancia de abstenerse de compartir demasiados detalles de los viajes (y cuánto tiempo estarán fuera de casa).

- Los puntos de acceso en hoteles, centros de conferencias y zonas públicas plantean importantes riesgos de seguridad (véase sección 4.5). Estas redes no suelen ser seguras, lo que permite a los piratas informáticos interceptar datos y, potencialmente, inyectar Malware en los dispositivos. Hay que evitar conectarse a Wi-Fi públicas y que, en su lugar, utilicen redes móviles seguras siempre que sea posible.

- La pérdida de datos puede ser devastadora, especialmente cuando se viaja. Haga hincapié en la importancia de realizar copias de seguridad (véase sección 4.4) periódicas de los archivos importantes, como fotos, vídeos, documentos y contactos. Se pueden emplear varios métodos, como servicios de almacenamiento en la nube, discos duros externos o USB.

- En zonas públicas como aeropuertos o cafeterías se deben evitar siempre dejar sus dispositivos desatendidos. Si es absolutamente necesario alejarse, los dispositivos deben bloquearse de forma segura con una contraseña y guardarse en un lugar seguro. Existen muchas bolsas antirrobo que pueden atarse de forma segura a los muebles si es necesario alejarse momentáneamente. Asegúrate de que las apps de rastreo están instaladas o activadas en los dispositivos que manejas para facilitar su recuperación en caso de robo o pérdida accidental.

Viajes Internacionales en una importante escalada de precauciones en los viajes internacionales, varios países aconsejan a sus ciudadanos para que utilicen teléfonos básicos y/o temporales y computadoras portátiles con datos mínimos al viajar a otros países, citando los crecientes temores de vigilancia digital y detenciones fronterizas arbitrarias. Las advertencias coordinadas reflejan la creciente preocupación por los informes de que agentes fronterizos de algunos países están inspeccionando dispositivos personales, accediendo a

datos privados y deteniendo a viajeros basándose en contenido digital, lo que ha provocado una ola de nuevos protocolos de viaje entre países.

Informes recientes han revelado inspecciones generalizadas de los dispositivos personales de los viajeros por las Oficina de Aduanas. Estos incluyen acceso no autorizado a correos electrónicos, cuentas de redes sociales, fotos y comunicaciones privadas, incluso en ausencia de una orden judicial penal. Este escrutinio ha provocado un aumento en el número de viajeros que son detenido, interrogado o se le negó la entrada al país basado en contenido digital encontrado durante la inspección.

En respuesta, varios gobiernos han actualizado sus directrices de viaje, advirtiendo a los ciudadanos que Llevar teléfonos inteligentes, computadoras portátiles o tabletas personales en viajes internacionales puede poner en riesgo su privacidad.

En el centro de los nuevos avisos se encuentra la recomendación explícita de utilizar teléfonos básicos y/o temporales y computadoras portátiles o tabletas reiniciadas a modo de fabrica. Estos teléfonos de bajo costo y con funciones limitadas permiten a los viajeros comunicarse y acceder a servicios esenciales sin exponer datos personales o profesionales confidenciales a los funcionarios fronterizos. Por otro lado, si se llevan computadoras portátiles o tabletas, estas se deben reiniciar a su versión de fabrica y llevar con datos mínimos usando cuentas temporales para su registro en dichos dispositivos (por ejemplo, usando una cuenta de Gmail/Apple temporal).

También se aconseja a los viajeros que:

- Realice una copia de seguridad de todos los datos en la nube y limpie los dispositivos antes de viajar.
- Evite almacenar información confidencial, política o profesional en cualquier Hardware.
- Borrar de forma permanente y segura datos personales de todos los dispositivos antes de viajar.
- Cerrar sesión en todas las cuentas personales y utilizar navegadores de incógnito si es necesario acceder.
- Evite iniciar sesión en cuentas personales de correo electrónico o redes sociales mientras se está en el extranjero.
- Usar almacenamiento en la nube encriptado en lugar de archivos locales.

- Minimizar el uso del dispositivo en la aduana para reducir la exposición.

Lo que una vez fue visto como paranoia se está convirtiendo rápidamente protocolo y los viajeros de todo el mundo se ven obligados a sopesar la conveniencia frente al control en un mundo cada vez más vigilado.

5 Meltdown, Spectre y lo que se Acumule

El tres de enero del 2018 se dio a conocer al público, que 6 meses antes se habían detectado dos distintos fallos en los procesadores de los equipos de cómputo, comunicaciones y redes de internet que usamos. Esto para dar tiempo a los desarrolladores de procesadores y de sistemas operativos de implementar estrategias para mitigar el problema. Estos son problemas de diseño de los procesadores de Intel, AMD, IBM POWER y ARM, esto significa que procesos con privilegios bajos (aquellos que lanzan las aplicaciones de usuarios convencionales) podían acceder a la memoria del Kernel del sistema operativo.

De los problemas detectados en el 2017, han seguido una larga sucesión de fallos encontrados por diversos investigadores hasta el día de hoy en múltiples procesadores actuales y anteriores. Un ataque que explotase dicho problema permitiría a un Software malicioso espiar lo que están haciendo otros procesos y también espiar los datos que están en esa memoria en el equipo de cómputo (o dispositivo móvil) atacado. En máquinas y servidores multiusuario, un proceso en una máquina virtual podría indagar en los datos de los procesos de otros procesos en ese servidor compartido.

Ese primer problema, es en realidad solo parte del desastre. Los datos actuales provienen especialmente de un grupo de investigadores de seguridad formados por expertos del llamado Project Zero[88] de Google. Ellos han publicado los detalles de dos ataques (no son los únicos[89]) basados en estos fallos de diseño. Los nombres de esos ataques son Meltdown y Spectre. Y en un sitio Web dedicado a describir estas vulnerabilidades destacaban que "aunque los programas normalmente no tienen permiso para leer datos de otros programas, un programa malicioso podría explotar Meltdown, Spectre y apropiarse de secretos almacenados en la memoria de otros programas".

[88] https://googleprojectzero.blogspot.com/

[89] Entre las distintas vulnerabilidades detectadas y sus variantes resaltan: Meltdown (AC, DE, P, SM, SS, UD, GP, NM, RW, XD, BR, PK, BND), Spectre (PHT, BTB, RSB, STL, SSB, RSRE), PortSmash, Foreshadow, Spoiler, ZombieLoad (1 y 2), Kaiser, RIDL, Plundervolt, LVI, Take a Way, Collide+Probe, Load+Reload, LVI-LFB, MSD, CSME, RYZENFALL (1, 2, 3, 4), FALLOUT (1, 2, 3) , CHIMERA (FW, HW), MASTERKEY (1, 2, 3), SWAPGS, ITLB_Multihit, SRBDS, L1TF, etc. Más información en:

https://cve.mitre.org
https://meltdownattack.com/

Como revelan en su estudio, la diferencia fundamental entre ambos es que Meltdown permite acceder a la memoria del sistema, mientras que Spectre permite acceder a la memoria de otras aplicaciones para robar esos datos.

En GNU/Linux, el Kernel (si usamos una versión actualizada) nos indica las fallas del procesador a las que es vulnerable, usando:

```
$ cat /proc/cpuinfo
lscpu
```

Ya que Meltdown y Spectre son problemas de diseño en los procesadores, no es posible encontrar solución por Hardware para los procesadores existentes y dado que constantemente aparecen nuevas formas de explotar dichos fallos, la única manera de mantener el equipo de cómputo, comunicaciones y redes de internet a salvo es mediante Software que debe implementar las soluciones en los sistemas operativos. En particular en el Kernel de Linux se trabaja en parchar en cada versión del Kernel todos los fallos reportados, por esto y por otra gama de fallos e inseguridades es necesario mantener siempre el sistema operativo y sus aplicaciones actualizadas.

Como se había comentado anteriormente, estos problemas de diseño afectan a todos los procesadores Intel, AMD, IBM POWER y ARM. Eso incluye básicamente a todos los procesadores que están funcionando al día de hoy en nuestros equipos, ya que estos procesadores llevan produciéndose desde 1995. Afecta a una amplia gama de sistemas.

En el momento de hacerse pública su existencia se incluían todos los dispositivos que no utilizasen una versión convenientemente parcheada de IOS, GNU/Linux, MacOS, Android, Windows y Android. Por lo tanto, muchos servidores y servicios en la nube se han visto impactados, así como potencialmente la mayoría de dispositivos inteligentes y sistemas embebidos que utilizan procesadores con arquitectura ARM (dispositivos móviles, televisores inteligentes y otros), incluyendo una amplia gama de equipo usado en redes. Se ha considerado que una solución basada únicamente en Software para estas fallas degrada el desempeño de los equipos de cómputo entre un 20 y un 40 por ciento dependiendo de la tarea que realizasen y el procesador del equipo.

5.1 ¿Qué es Meltdown?

este fallo explota una condición de carrera inhe-rente al diseño de muchas CPU actuales. Esta condición se da entre los accesos a la memoria y la comprobación de privilegios durante el procesamiento de instrucciones. Además, en combinación con un ataque de canal lateral a la memoria caché de la CPU, esta vulnerabilidad permite que un proceso se salte las comprobaciones habituales de nivel de privilegio que normalmente aislarían al proceso maligno e impedirían que accediese a datos que pertenecen al sistema operativo y otros procesos concurrentes.

La vulnerabilidad permite que un proceso no autorizado lea información de cualquier dirección mapeada al espacio de memoria del proceso actual. Dado que la segmentación de instrucciones reside en los procesadores afectados, la información de una dirección no autorizada casi siempre se cargará temporalmente en la memoria caché de la CPU durante la ejecución fuera de orden, pudiendo posteriormente leerse desde la memoria caché. Esto puede suceder incluso cuando la instrucción de lectura original falla debido a una comprobación de privilegios que da negativo, o cuando no produce un resultado legible.

Dado que muchos sistemas operativos mapean la memoria física, los procesos del núcleo y otros procesos del espacio de usuario en el espacio de direcciones de cada proceso, Meltdown permite que un proceso maligno pueda leer cualquier memoria mapeada física, del núcleo o de otro proceso, con independencia de si debería o no poder hacerlo. Las defensas contra Meltdown exigirían evitar el uso del mapeo de memoria de un modo que resultase vulnerable a tales amenazas (una solución basada en Software), o bien evitar la condición de carrera subyacente (una modificación del microcódigo de la CPU o la ruta de ejecución).

El agujero es viable en cualquier sistema operativo en el que la información privilegiada se mapea a memoria virtual para procesos no privilegiados, una característica que incorporan muchos sistemas operativos actuales. Por lo tanto, potencialmente Meltdown puede afectar a una gama de dispositivos mayor que la identificada actualmente, dado que apenas hay variaciones entre las familias de microprocesadores utilizados por estos sistemas.

5.2 ¿Qué es Spectre?

es una vulnerabilidad que permite a los programas alojados en el sistema operativo del usuario acceder a una dirección arbitraria del espacio de memoria de un programa. En lugar de una única vulnerabi-lidad de fácil corrección, el documento de Spectre describe una clase entera de vulnerabilidades potenciales. Todas esas vulnerabilidades se basan en explotar los efectos secundarios de la ejecución especulativa, una técnica empleada comúnmente para combatir la latencia de la memoria y acelerar así la ejecución en los microprocesadores modernos.

En particular, Spectre se centra en la predicción de saltos, un caso especial de la ejecución especulativa. A diferencia de la vulnerabilidad Meltdown hecha pública la misma fecha, Spectre no depende de una característica en particular de la gestión de memoria de un procesador en concreto o de cómo proteja el acceso a esa memoria, sino que tiene un enfoque más general.

El punto de partida del documento de Spectre es un ataque sincronizado de canal lateral aplicado al sistema de predicción de saltos de un microprocesador moderno que utilice ejecución fuera de orden. Si bien al nivel arquitectónico documentado en las hojas técnicas de los procesadores los resultados de un fallo en la predicción se especifican que quedarán anulados tras darse dicha circunstancia, la ejecución especulativa resultante puede aun así dejar efectos colaterales, como líneas de caché cargadas con determinada información.

Estos efectos colaterales pueden posteriormente afectar a los denominados aspectos no funcionales del sistema informático. Si tales efectos colaterales -incluyendo, entre otros, los tiempos de acceso a la memoria- resultan visibles para un programa malicioso, y puede hacerse que esos efectos dependan de información sensible en posesión del proceso que hace las veces de víctima, entonces estos efectos colaterales pueden hacer que la información sensible resulte deducible. Esto puede ocurrir aunque los sistemas de seguridad formales a nivel de arquitectura funcionen de forma correcta -lo que sucede es que las optimizaciones en los niveles más bajos a nivel de microarquitectura dirigidas a la aceleración la ejecución de código pueden revelar información no esencial para la correcta ejecución de un programa-.

5.3 Falla en los Procesadores Snapdragon

El día 8 de agosto del 2020 se público que los procesadores Qualcomm Snapdragon[90] de más de 3 mil millones de dispositivos Android del mundo son vulnerables a ataques que pueden convertirlos en herramientas de espionaje al explotar más de cuatrocientas vulnerabilidades y no se sabe cuando Google y los fabricantes de dispositivos móviles incorporarán la solución de Qualcomm.

Las vulnerabilidades pueden explotarse cuando un objetivo descarga un video u otro contenido que es procesado por el Chip. Los objetivos también pueden ser atacados instalando aplicaciones maliciosas que no requieren ningún permiso. Desde allí, los atacantes pueden monitorear ubicaciones y escuchar audio cercano en tiempo real y filtrar fotos y videos. Las infecciones se pueden ocultar del sistema operativo de tal manera que dificulta la desinfección.

Snapdragon es lo que se conoce como un sistema en un Chip que proporciona una gran cantidad de componentes, como una CPU y un procesador de gráficos. Una de las funciones conocida como procesamiento de señal digital o DSP, aborda una variedad de tareas, incluidas las capacidades de carga y de las funciones de video, audio, realidad aumentada y otras funciones multimedia.

Los investigadores de la firma de seguridad Check Point en un breve informe sobre las vulnerabilidades que descubrieron indican que estos Chips introducen una nueva superficie de ataque y puntos débiles en estos dispositivos móviles por las múltiples vulnerabilidades de los DSP. Qualcomm ha lanzado una solución a las fallas, pero hasta el momento no se han incorporado al sistema operativo Android.

Por el momento Check Point está reteniendo detalles técnicos sobre las vulnerabilidades y cómo se pueden explotar hasta que las soluciones lleguen a los dispositivos del usuario final. Check Point ha denominado a las vulnerabilidades Achilles. Los más de 400 errores distintos se rastrean como:

> CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208 y CVE-2020-11209.

En un comunicado, los funcionarios de Qualcomm dijeron: "Con respecto a la vulnerabilidad de Qualcomm Compute DSP revelada por Check Point,

[90] Representa a más del 40% de los teléfonos inteligentes del mercado incluyendo a los teléfonos de las compañías Google, Samsung, LG, Xiaomi, OnePlus, Motorola, etc.

trabajamos diligentemente para validar el problema y poner las mitigaciones adecuadas a disposición de los OEM. No tenemos evidencia de que esté siendo explotado actualmente. Alentamos a los usuarios finales a actualizar sus dispositivos a medida que los parches estén disponibles y solo a instalar aplicaciones de ubicaciones confiables como Google Play Store".

No hay mucha orientación útil para proporcionar a los usuarios cómo protegerse contra estos ataques. Descargar aplicaciones sólo desde Play puede ayudar, pero el historial de verificación de aplicaciones de Google muestra que los consejos tienen una eficacia limitada. Tampoco hay forma de identificar eficazmente el contenido multimedia explotable.

5.4 Falla en el Chip T2 de las Mac

Expertos en ciberseguridad de la empresa belga *ironPeak* han confirmado los rumores de que los Chips de seguridad T2 pueden llegar a ser Hackeados: una determinada combinación de dos 'exploits' diferentes proporciona al atacante la oportunidad no sólo de cambiar el comportamiento del Chip, sino incluso de instalar Malware en el mismo (como keyloggers).

Y hay tres factores que hacen que esta noticia resulte especialmente chocante... y preocupante:

- Que el objetivo de estos Chips T2 es precisamente el de salvaguardar la seguridad de los datos: se trata de un procesador independiente que actúa de intermediario entre la CPU y el sistema operativo y que permite supervisar que sólo se ejecute en el equipo Software aprobado por Apple.

- Que el Chip T2 viene instalado en todos los iMac Pro, Macbook Pro y Macbook Air vendidos desde 2018, en todos los Mac Pro desde 2019 y en todos los iMac del 2020. Es decir, afecta a un número notable de usuarios.

- Pero lo peor de todo es que, aunque el atacante puede modificar el comportamiento del Chip T2, la vulnerabilidad no puede ser parcheada preventivamente, porque ésta se basa precisamente en la escritura del apartado de sólo lectura del Chip.

¿Cómo Funciona este Ataque? los Exploits usados para esta clase de ataque son dos que ya se venían usando para aplicar el Jailbreak a dispositivos iOS (el T2 está basado en el Chip A10, usado por los iPhones más antiguos). Según *ironPeak*, este método funciona porque: "Apple dejó abierta una interfaz de depuración cuando envió los Chips T2 a los clientes, lo que permite a cualquiera entrar en el modo de actualización de Firmware del dispositivo sin autenticación".

Con este método, es posible crear un cable USB-C que puede explotar automáticamente la vulnerabilidad de su dispositivo MacOS durante el arranque. Esto permite a un atacante obtener acceso *root* sobre el Chip T2 y modificar o controlar cualquier cosa que se ejecute en el dispositivo atacado.

El lado bueno de esto es que, como habrás deducido de leer lo anterior, esta clase de ataque requiere de acceso físico para funcionar (idealmente, de varios accesos físicos). En principio, el riego para un usuario medio de Mac es bastante bajo (otra cosa son aquellos equipos integrados en redes de grandes empresas y organismos públicos).

Ante la imposibilidad de parchearlo, desde *ironPeak* se muestran convencidos de que Apple desarrollará una nueva versión del T2 para los próximos equipos que lance al mercado... la cual dejará de ser necesaria cuando desembarque la próxima generación Apple Silicon, que traerá incluidas las funciones de seguridad en el propio Chip ARM.

5.5 Falla en el Chip M1 de las Mac

Los Chips M1 de Apple tienen una vulnerabilidad de Hardware "no parcheable" que podría permitir a los atacantes atravesar su última línea de defensas de seguridad, según descubrieron los investigadores del MIT.

La vulnerabilidad radica en un mecanismo de seguridad a nivel de Hardware utilizado en los Chips Apple M1 llamados códigos de autenticación de puntero o PAC. Esta característica hace que sea mucho más difícil para un atacante inyectar código malicioso en la memoria de un dispositivo y proporciona un nivel de defensa contra las explotaciones de desbordamiento de búfer, un tipo de ataque que obliga a que la memoria se derrame en otras ubicaciones del Chip.

Sin embargo, los investigadores del Laboratorio de Ciencias de la Computación e Inteligencia Artificial del MIT han creado un nuevo ataque de Hardware, que combina la corrupción de la memoria y los ataques de ejecución especulativa para eludir la función de seguridad. El ataque muestra que

la autenticación de puntero puede anularse sin dejar rastro y, dado que utiliza un mecanismo de Hardware, ningún parche de Software puede solucionarlo.

El ataque, apropiadamente llamado "Pacman", funciona al "adivinar" un código de autenticación de puntero (PAC), una firma criptográfica que confirma que una aplicación no ha sido alterada de manera maliciosa. Esto se hace mediante la ejecución especulativa, una técnica utilizada por los procesadores informáticos modernos para acelerar el rendimiento al adivinar especulativamente varias líneas de cálculo, para filtrar los resultados de verificación de PAC, mientras que un canal lateral de Hardware revela si la suposición fue correcta o no.

Además, dado que solo hay una cantidad limitada de valores posibles para el PAC, los investigadores descubrieron que es posible probarlos todos para encontrar el correcto.

En una prueba de concepto, los investigadores demostraron que el ataque incluso funciona contra el Kernel, el núcleo de Software del sistema operativo de un dispositivo, lo que tiene "implicaciones masivas para el trabajo de seguridad futuro en todos los sistemas ARM con autenticación de puntero habilitada", dice Joseph Ravichandran, estudiante de doctorado en MIT CSAIL y coautor principal del artículo de investigación.

"La idea detrás de la autenticación de puntero es que si todo lo demás ha fallado, aún puede confiar en él para evitar que los atacantes obtengan el control de su sistema", agregó Ravichandran. "Hemos demostrado que la autenticación de puntero como última línea de defensa no es tan absoluta como alguna vez pensamos que era".

Apple ha implementado la autenticación de puntero en todo su silicio basado en ARM personalizado hasta el momento, incluidos el M1, M1 Pro y M1 Max, y varios otros fabricantes de Chips, incluidos Qualcomm y Samsung, han anunciado o se espera que envíen nuevos procesadores. compatible con la función de seguridad a nivel de Hardware. MIT dijo que aún no ha probado el ataque en el Chip M2 inédito de Apple, que también admite autenticación de puntero.

"Si no se mitiga, nuestro ataque afectará a la mayoría de los dispositivos móviles y probablemente incluso a los dispositivos de escritorio en los próximos años", dijo el MIT en el documento de investigación.

Los investigadores, que presentaron sus hallazgos a Apple, señalaron que el ataque de Pacman no es un "desvío mágico" para toda la seguridad en el Chip M1, y solo puede tomar un error existente contra el que protege la autenticación de puntero.

Cuando se contactó antes de la publicación en Junio del 2022, Apple no quiso comentar sobre el registro. Después de la publicación, el portavoz de Apple, Scott Radcliffe, proporcionó lo siguiente: "Queremos agradecer a los investigadores por su colaboración, ya que esta prueba de concepto avanza en nuestra comprensión de estas técnicas. Según nuestro análisis, así como los detalles compartidos con nosotros por los investigadores, hemos concluido que este problema no representa un riesgo inmediato para nuestros usuarios y es insuficiente para eludir las protecciones de seguridad del sistema operativo por sí solo".

En mayo del 2022, un desarrollador descubrió una falla irreparable en el Chip M1 de Apple que crea un canal encubierto que dos o más aplicaciones maliciosas ya instaladas podrían usar para transmitir información entre sí. Pero el error finalmente se consideró "inofensivo" ya que el Malware no puede usarlo para robar o interferir con los datos que están en una Mac.

5.6 GhostRace

es un ataque de ejecución especulativa que afecta a procesadores Intel, AMD, ARM e IBM (catalogado bajo CVE-2024-2193), este es un nuevo método desarrollado por investigadores de la Vrije Universiteit Amsterdam e IBM para explotar el mecanismo de ejecución especulativa presente en procesadores modernos de Intel, AMD, ARM e IBM.

Los investigadores mencionan que, GhostRace se enfoca en manipular condiciones de carrera especulativas para acceder a áreas de memoria previamente liberadas, lo que puede llevar a la extracción de datos sensibles del Kernel de Linux, especialmente en entornos de virtualización donde un atacante en un sistema invitado puede comprometer la seguridad del sistema anfitrión o de otros sistemas invitados.

El funcionamiento documentado del ataque se basa en la ejecución especulativa de instrucciones condicionales con primitivas de sincronización de subprocesos, como Mutex y Spinlock. Si el procesador predice incorrectamente ramas en el código que manejan estas operaciones, se pueden realizar accesos especulativos a la memoria que ya ha sido liberada. Aunque el procesador descarta estos accesos después de detectar la predicción errónea, los rastros de ejecución permanecen en la memoria caché y pueden ser recuperados mediante técnicas de análisis de canal lateral.

GhostRace requiere la presencia de ciertas secuencias de instrucciones en el kernel, conocidas como Gadgets, que son utilizadas para la ejecución es-

peculativa dependiendo de condiciones externas controladas por el atacante. Estos Gadgets se forman a partir de secciones de código donde se verifica el estado en un bucle sin fin y se sale del bucle después de eliminar el bloqueo de acceso al recurso. Esto permite activar falsamente una transición y ejecutar instrucciones protegidas por un bloqueo, a pesar de que el recurso permanece bloqueado.

Durante el análisis de la vulnerabilidad, que se realizó en el código del kernel de Linux 5.15.83, se reveló la presencia de 1283 dispositivos que podrían conducir a un acceso especulativo a la memoria ya liberada. Este tipo de ataque representa un riesgo potencial para sistemas de virtualización, cualquier Kernel del sistema operativo y programas que utilicen primitivas de sincronización de subprocesos verificadas mediante declaraciones condicionales y se ejecuten en plataformas que permitan la ejecución especulativa de operaciones de ramificación, como x86, ARM, RISC-V, entre otros.

Para probar la vulnerabilidad, los investigadores desarrollaron un prototipo de Exploit que demuestra la efectividad del ataque al permitir la extracción de datos de la memoria del kernel de Linux con un rendimiento de 12 KB por segundo y un nivel de confiabilidad similar a los ataques de la clase Spectre.

Los desarrolladores del Kernel de Linux y las empresas de fabricación de CPU fueron informados sobre este problema a finales de 2023. AMD ya ha publicado un informe sobre la vulnerabilidad y recomienda el uso de técnicas estándar para protegerse contra ataques similares a Spectre v1. Por otro lado, Intel y ARM aún no han respondido a esta notificación.

Aunque los desarrolladores del kernel de Linux no tienen planes inmediatos de implementar la serialización de primitivas de sincronización debido a la pérdida de rendimiento, ya han incorporado restricciones para protegerse contra la técnica de explotación IPI Storming (CVE-2024-26602). Esta técnica de ataque implica interrumpir un proceso en el momento adecuado para proporcionar una ventana de tiempo para el acceso especulativo a la memoria liberada.

Para mitigar este tipo de ataque, se propone utilizar la serialización de primitivas de sincronización mediante la inclusión de una instrucción LFENCE después de la instrucción cmpxchq que verifica el estado de bloqueo. Sin embargo, esta medida de protección conlleva una penalización de rendimiento de aproximadamente el 5 % en el punto de referencia LMBench, debido a que la instrucción LFENCE deshabilita la ejecución preventiva de instrucciones posteriores antes de confirmar todas las operaciones anteriores.

5.7 Caballo de Troya de Hardware

o Hardware Trojan Horse (HTH), es una modificación malintencionada en un circuito integrado para usarlo con fines de espionaje, destruir el sistema, accesos no autorizados, o para alterar el funcionamiento de una máquina para algún otro fin, eludiendo los sistemas de seguridad o desactivando éstos. Un HTH está constituido por:

- Representación física: es la parte del Hardware Trojan compuesta por una serie de alteraciones en el circuito. Estas modificaciones pueden ser:

  ◦ Funcional: si se han modificado algunos transistores o puertas lógicas del circuito original para implementar otro circuito diferente, o que continúe prestando el mismo servicio con algunas funciones ocultas extra. Además, el encapsulado camufla estas modificaciones, haciendo que el Chip sea exactamente idéntico en aspecto. Incluso si se analiza el Die Shot para comparar cambios en la superficie ocupada por la lógica maliciosa, la detección es complicada, ya que en muchos casos no crece el área, sino que simplemente son cambios estructurales. Realiza ingeniería inversa, estudiar termografías, sondas lógicas, etc., tampoco es garantía de detectar el problema, ya que en algunas ocasiones se pueden camuflar usando circuitería BIST, su E/S aparentemente responde de forma normal si no se ha activado, o no se altera demasiado la potencia disipada. En ocasiones, cuando se activan, sí que se pueden apreciar cambios en el consumo eléctrico del Chip. Por otro lado, la distribución del troyano puede hacerse mediante:

    · Loose distribution (distribución suelta): cuando los componentes del troyano están dispersos en varios Chips de la máquina.
    · Tight distribution (distribución ajustada): se concentra en un único circuito integrado, puesto que el área necesaria para su implementación no es demasiado grande.

  ◦ Paramétrico: se modifica el circuito original sin alterar la lógica, solo adelgazando algunas interconexiones, debilitando transistores, etc. Para ello, se somete el circuito integrado a radiación o se usa FIB (Focused Ion-Beams). Esto haría que el Chip no sea

fiable y pueda fallar, lo que podría ser nefasto si se está usando para aplicaciones críticas.

- Sistema de activación: un Hardware Trojan también necesitará de un sistema necesario para detectar ciertas condiciones para activar la función para la que haya sido creado. Puede ser mediante sensores, cuando detecta ciertos estados lógicos internos, secuenciales o combinacionales, cuando llega a un patrón determinado de cómputo, mediante un contador o temporizador, etc. Por ejemplo, podría usarse para detectar pulsaciones de teclado como un Keylogger para capturar contraseñas, que dados unos estados lógicos en un bus generar un código que produzca un mal funcionamiento del sistema, estar en sistemas de control de misiles para que el enemigo pueda desactivarlos a distancia cuando se activan estas armas, en maquinaria industrial para reportar datos para el espionaje, introducir una puerta trasera, etc.

- Accionador: una cosa es el sistema encargado de analizar las condiciones para la activación, y otra distinta la parte que acciona y genera la función maliciosa. Esta parte es la que desencadena realmente el ataque o la función para filtrar información confidencial, generar errores o funcionamiento anómalo, dar acceso remoto o permitir el control del atacante, etc.

- Auxiliares: un troyano de Hardware también puede disponer de ciertas partes periféricas necesarias para su funcionamiento. Estos periféricos variarán enormemente en función de los objetivos de cada troyano, e incluso se podrían usar las mismos componentes funcionales de la máquina para estos fines. Por ejemplo, la memoria principal para almacenar datos, la tarjeta de red para comunicaciones, etc.

Detección de los Hardware Trojan Estos troyanos de Hardware pueden permanecer latentes, pero una vez activos, pueden causar problemas muy graves, comprometiendo la funcionalidad de un sistema, filtrando información confidencial, etc. Eso unido a lo «sigilosos» que son los hace potencialmente peligrosos. Las técnicas tradicionales no son suficientes, y la cantidad de tecnología empleada en la actualidad hace complicado que se analicen todos y cada uno de los dispositivos empleados.

A pesar de eso, existen varias formas empleadas para detectar este tipo de Hardware Trojan, algunas ya las he citado anteriormente. Estas técnicas

suelen ser similares a las que se emplean en la industria de los semiconductores para probar los Chips:

- Inspección física: se inspeccionan cosas desde las más transcendentales, como el número de pines, mediciones del área, hasta otras más profundas desencapsulando el Chip y empleando técnicas de termografía, análisis de consumo, microscopía óptica (MO), barrido SEM (Scanning Electron Microscopy), análisis PICA (Picosecond Imaging Circuit Analysis), inspección de imágenes VCI (Voltage Contrast Imaging), técnicas LIVA (Light-induced Voltage Alteration), FANCI (Functional Analysis for Nearly-unused Circuit Identification), y CIVA (Charge-Induced Voltage Alteration). Por ejemplo, las técnicas FANCI, que parecían muy prometedoras, mediante un análisis booleano estático para etiquetar las conexiones que pueden ser potencialmente maliciosas, ha resultado también poco efectivo, ya que se puede hacer que el diseño del troyano de Hardware parezca más benigno ante este tipo de técnicas.

- Test funcional: se usan sondas lógicas para generar una serie de estados en las entradas de un circuito y se monitorizan los estados de la salida, para detectar posibles alteraciones en los patrones.

- BIST (Built-in self-test) y DFT (Design For Testing): en los Chips se suele emplear una lógica adicional para verificar la funcionalidad de un circuito o si tiene defectos. Pero estos pueden haber sido alterados para camuflar estos cambios. Los Chips originales generan una firma determinada, pero si está alterado generaría una firma desconocida con estas pruebas. Pero es como cuando compruebas una suma de verificación de un Software... ¿y si la han alterado también?

- Análisis del canal lateral: los circuitos integrados activos emiten señales como campos magnéticos y eléctricos concretos (como una especie de firma también, véase el ejemplo de los Side-channel Attacks). Esas señales son causadas por la actividad eléctrica del Chip, por lo que pueden ser estudiados para obtener información, al igual que se puede emplear una termografía.

Casos reales este tipo de troyanos pueden afectar a multitud de circuitos muy diferentes, desde procesadores, hasta memoria, pasando por otros

circuitos integrados de los sistemas de computación y del internet de las cosas (con su crecimiento exponencial). Y su origen de estas «falsificaciones» pueden provenir de múltiples fuentes, desde las propias fábricas donde se producen, hasta la modificación de piezas que necesitan post-procesamiento en el extranjero.

Algunos reportes gubernamentales, como uno realizado por el gobierno de EE.UU. de 2012, detectó varios casos de circuitos integrados modificados que se habían infiltrado en la cadena de suministro del sistema de defensa de ese país. Y cada vez son más frecuentes.

A lo largo de la historia también se han usado varios ataques basados en un Hardware Trojan. Uno muy conocido es el que se produjo en Irak cuando Estados Unidos envió impresoras con un Chip modificado en 1991. Estas impresoras incluían un sistema que les permitirían expandir un malware en los sistemas operativos Windows conectados a estas impresoras con el objetivo de apagar las instalaciones de los radares.

6 Distribuciones Seguras, Penetración, Inmutables y IOT

Para muchos, Linux y Mac OS son dos sistemas operativos más seguros que Windows de Microsoft, pero con todo, hay algunas distribuciones especializadas de Linux que satisfacen las necesidades de temas relacionados con la seguridad, pruebas de penetración, análisis forense, auditorías de seguridad, etc.

Las distribuciones seguras intentan preservar la privacidad y el anonimato, ayudan a utilizar internet de forma anónima y evitar la censura en prácticamente cualquier lugar y cualquier equipo de cómputo, pero sin dejar rastro a menos que lo solicites explícitamente.

Las distribuciones para pruebas de penetración ofrecen herramientas para penetración, análisis forense y auditorías de seguridad en donde se realizan distintos tipos de tareas que identifican, en una infraestructura objetivo, las vulnerabilidades que podrían explotarse y los daños que podría causar un atacante. En otras palabras, se realiza un proceso de Hacking ético para identificar qué incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de tal forma que se eviten estos ataques.

Además, las distribuciones anónimas ofrecen niveles adicionales de privacidad y seguridad y se complementan con las distribuciones para pruebas de penetración que ofrecen herramientas para penetración y auditorías de seguridad (mediante el uso de tecnologías como TOR[91], Sandbox[92], Firewall[93],

[91] Tor es una red abierta y distribuida que te ayuda a defenderte de una forma de vigilancia en la red que amenaza tu libertad y privacidad, tus actividades comerciales confidenciales y relaciones, además de la seguridad gubernamental. Además, te protege redirigiendo tus comunicaciones alrededor de una red distribuida de retransmisores realizados por voluntarios alrededor del mundo: lo cual previene que alguien observe tus comunicaciones a partir de los sitios que visitas, también evita que los sitios en que navegas obtengan tu ubicación física.

[92] Sandbox es un mecanismo para ejecutar programas con seguridad y de manera separada. A menudo se utiliza para ejecutar código nuevo, o Software de dudosa confiabilidad proveniente de terceros. Ese entorno aislado permite controlar de cerca los recursos proporcionados a los programas cliente a ejecutarse, tales como espacio temporal en discos y memoria. Habitualmente se restringen las capacidades de acceso a redes, la habilidad de inspeccionar la máquina anfitrión y dispositivos de entrada entre otros. En este sentido, el aislamiento de procesos es un ejemplo específico de virtualización.

[93] Un cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata

herramientas criptográficas[94], etc.). De ambos tipos de Softwares hay varias alternativas diferentes, tanto comerciales como de Software libre, por lo que decidirse por una u otra, en ocasiones puede ser una tarea un tanto complicada. Es por ello que aquí listamos algunas de las distribuciones de Linux más usadas en la actualidad, apartados con los que cada vez debemos prestar más atención.

Las distribuciones inmutables garantizan que el núcleo del sistema operativo permanezca sin cambios. El sistema de archivos raíz de una distribución inmutable sigue siendo de solo lectura, lo que permite permanecer igual en varias instancias (por supuesto, puedes cambiar las cosas si así lo deseas, sin embargo, la capacidad permanece desactivada de forma predeterminada).

Por otro lado, existen versiones de sistemas operativos para el Internet de las cosas (IOT), estos sistemas operativos están diseñado específicamente para funcionar dentro de las limitaciones particulares de los dispositivos de IoT, que generalmente están limitados en tamaño de memoria, potencia de procesamiento y capacidad, y están diseñados para permitir una transferencia rápida de datos a través de Internet. Hay varios sistemas operativos (principalmente basados en Linux) que puedes usar para IoT, pero no te permitirán aprovechar al máximo tu configuración y esa es la razón por la que existen distribuciones centradas en IoT.

Algunas de las distribuciones seguras, para penetración e inmutables son sistemas operativos Live[95] diseñados para ser usados desde un CD, DVD,

de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de internet no autorizados tengan acceso a redes privadas, especialmente intranets.

[94] El surgimiento de redes de comunicación, en particular de internet, ha abierto nuevas posibilidades para el intercambio de información. Al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite. Es necesario entonces, crear diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos, todo ello es parte de la Criptografía.

[95] Un Live CD/DVD o USB, más genéricamente Live Distro, es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD/DVD o USB (de ahí sus nombres), que puede ejecutarse directamente en una computadora.

En la historia más reciente de Linux, las llamadas distribuciones Live Distro se han vuelto muy populares porque le permiten probar una distribución de Linux sin siquiera instalarla en el equipo. Esto es excelente porque no tiene todas las molestias de volver a particionar el disco o instalarlo sobre su sistema operativo (Windows/Mac OS). Simplemente puede colocar el CD/DVD o USB para una distribución en vivo e iniciar la computadora desde ahí. Por lo general, obtiene la mayor parte de la funcionalidad princi-

memoria USB o máquina virtual independientemente del sistema operativo original de la computadora.

6.1 Distribuciones de GNU/Linux «Seguras»

Tails (https://tails.boum.org/)

Para muchos esta es la primera opción a la hora de buscar una solución de seguridad en Linux. También conocida como «The Amnesic Incognito Live System», esta es una distribución basada en Debian GNU/Linux . Es un proyecto de código abierto que se publicó por primera vez hace 8 años y que redirige todo el tráfico Web a través de Tor logrando la privacidad a través del anonimato. Además, almacena todo en la RAM y evita el uso del disco duro, por lo que borra todo una vez se apaga. La imagen tiene un tamaño menor de 1.2 GB y necesita al menos 2 GB de RAM en un equipo de 64 bits, se puede usar en formato Live, como máquina Virtual o bien instalarse en una USB, DVD o en el disco duro del equipo.

Septor (https://septor.sourceforge.io)

Es un sistema operativo que proporciona a los usuarios un entorno informático perfecto para navegar por internet de forma anónima. Septor proporciona a los usuarios una distribución estable y confiable que se basa en

pal de la distribución, por lo que realmente puede evaluar si la distribución es para usted antes de elegir instalarla de verdad.

Normalmente, una versión Live viene acompañado de un par de aplicaciones. Algunos Live CD/DVD o USB incluyen una herramienta que permite instalarlos en el disco duro. Otra característica es que por lo general no se efectúan cambios en la computadora utilizada.

Para usar una versión Live es necesario obtener uno (muchos de ellos distribuyen libremente una imagen ISO que puede bajarse de Internet y grabarse en disco/USB) y configurar la computadora para que arranque desde la unidad lectora, reiniciando luego la computadora con el disco en la lectora o USB, con lo que el que el sistema Live se iniciará manualmente.

Uno de los mayores inconvenientes de este sistema es el mal uso de una gran cantidad de memoria RAM, una parte para su uso habitual y otra para funcionar como el disco virtual del sistema. En el arranque, se le pueden dar distintos parámetros para adaptar el sistema a la computadora, como la resolución de pantalla o para activar o desactivar la búsqueda automática de determinado Hardware.

Otro inconveniente es el rendimiento de la Live Distro, pues la velocidad de transferencia de las unidades lectoras CD/DVD o USB es muy inferior a la de los discos duros. Una vez instalada en la computadora se apreciará la velocidad real de la distribución.

Debian GNU/Linux y funciona en una amplia gama de computadoras, usa un escritorio KDE Plasma personalizado y tecnologías Tor. Esta distribución es similar a Tails y se puede usar en vivo directamente desde una unidad Flash USB, máquina virtual o instalarla localmente.

Whonix (https://www.whonix.org/)

Es una distribución que se basa en Debian GNU/Linux y consta de dos máquinas virtuales, una es Tor Gateway que se ejecuta en Debian GNU/Linux, mientras que la otra es una Workstation. Whonix se instala en un sistema operativo Host proporcionado por el usuario que puede ser Linux, Windows, MacOS o Qubes OS. Así al utilizar la red abierta y distribuida de transmisión de Tor, Whonix echa abajo las posibilidades de vigilancia de la Red. Además, y por motivos de seguridad, hace todo lo posible para ocultar nuestra dirección IP real.

Qubes OS (https://www.qubes-os.org/)

Se conoce como uno de los sistemas operativos más seguros del mundo y se basa en realizar la virtualización mediante el «hipervisor Xen» -un hipervisor imita el Hardware y permite ejecutar varias máquinas virtuales simultáneamente-. El entorno de usuario de Qubes OS podría ser Fedora, Debian, Whoix o Windows y, al igual que Tails. Así mismo utiliza diferentes dominios para separar los niveles de confianza, por ejemplo, un dominio de trabajo, un dominio para el ocio, etc.; los cuales se ejecutan en diferentes máquinas virtuales, esta versión requiere un mínimo de 16 GB de RAM.

Subgraph OS (https://subgraph.com/)

Nos encontramos con un sistema operativo seguro basado en Debian GNU/Linux que promete proporcionar una experiencia digital anónima. Ha sido diseñado para evitar diferentes ataques de Malware, es capaz de ser una plataforma de comunicación segura además de proporcionar una interfaz de usuario muy sencilla.

Discreete Linux (https://www.privacy-cd.org/)

En este caso nos encontramos con un proyecto de Software libre que puede ser utilizado por cualquier persona que desee llevar una vida digital anónima también basado en Debian GNU/Linux. Además, protege a sus usuarios contra los ataques de vigilancia accionados por troyanos. Es una de las

alternativas más adecuadas para los usuarios que no tienen un conocimiento muy profundo de estos sistemas pero que consideran la seguridad en internet como su principal preocupación. Hace uso de cifrados y entornos aislados para proporcionar un entorno de trabajo seguro. Así mismo no utiliza los discos duros internos del equipo, ya que almacena todos sus datos en la memoria RAM o en una unidad de disco USB externa.

Kodachi (https://www.digi77.com/linux-kodachi/)
Es un sistema operativo centrado en la seguridad y basado en Debian GNU/Linux cuyo objetivo es proporcionar una experiencia informática segura. Ponerlo en marcha es muy sencillo y no necesita demasiado tiempo, ya que permite la opción de arrancar desde el Hardware del PC, o desde una unidad USB externa para mayor seguridad. Hace uso de elementos tales como una conexión VPN activa, el servicio TOR y DNScrypt con el que garantiza un buen nivel de privacidad. Además, todo el sistema operativo se ejecuta desde la memoria RAM del equipo, por lo que después de apagado no queda ningún rastro de actividad.

Tens (https://www.spi.dod.mil/lipose.htm)
También conocido como Trusted End Node Security, este sistema es distribuido y desarrollado por el Departamento de Defensa de los Estados Unidos. Se basa en Arch Linux y puede ejecutarse en cualquier equipo con tecnología Intel. Sólo arranca desde la RAM y viene cargado con un asistente de cifrado, un Software de cifrado simple y potente para la protección de nuestra información confidencial.

Tin Hat (https://sourceforge.net/projects/tinhat/)
Esta propuesta es una derivación de Gentoo y es un sistema operativo seguro que se ejecuta en su totalidad en la RAM del equipo, por lo que no monta ningún sistema de archivos directamente en el dispositivo de arranque, evitando así la posibilidad de dejar expuesto cualquier dato. Como era de esperar, podremos arrancarlo desde un CD o desde una unidad flash USB. Puede ejecutarse tanto en arquitecturas de Hardware de 32 como de 64 bits y es recomendable tener conocimientos previos de Gentoo Linux.

IprediaOS (https://www.ipredia.org/os/)

Para empezar diremos que I2P es una capa de comunicación P2P anónima que se crea utilizando herramientas de código abierto, algo en lo que se basa IprediaOS, ya que orienta todo su tráfico a través de I2P y se asegura de que toda su actividad Online no pueda ser interceptada por terceros. Así hace uso de múltiples capas de cifrado y cabe mencionar que la red I2P es una red dinámica y distribuida.

Alpine Linux (https://alpinelinux.org/)
Es una distribución diseñada principalmente para los usuarios avanzados que valoran la seguridad, la eficiencia de recursos y la simplicidad. En un principio parte como bifurcación del proyecto *LEAF* aunque, a diferencia de este, Alpine mejora las características de seguridad y cuenta con un Kernel más actual. Su funcionamiento se centra en la privacidad, por lo que utiliza su propio sistema de gestión de paquetes.

Openwall (https://www.openwall.com/Owl/)
Es una pequeña distribución de Linux con seguridad mejorada (SELinux) para servidores, dispositivos y dispositivos virtuales. A diferencia de otras distribuciones, el uso de SELinux por parte de Openwall evita que se incorpore Software vulnerable a la distribución, en lugar de depender de parches para remediar vulnerabilidades de seguridad conocidas o características diseñadas para disminuir el impacto de los errores de seguridad. Mediante el uso del marco *SELinux*, Openwall eclipsa a la mayoría de sus contrapartes más grandes en este sentido.

6.2 Distribuciones de GNU/Linux «Para Penetración»

Realizar pruebas de penetración, análisis forense y auditorías de seguridad resulta ser una tarea compleja e involucra un proceso en donde se realizan distintos tipos de tareas que identifican, en una infraestructura objetivo, las vulnerabilidades que podrían explotarse y los daños que podría causar un atacante. En otras palabras, se realiza un proceso de Hacking ético para identificar qué incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de tal forma que se eviten estos ataques.

Para realizar una prueba de penetración de forma profesional, es necesario sumar a los conocimientos de Hacking ético, otros aspectos fundamentales como: programación, metodologías, documentación, entre otros. No

obstante, esos aprendizajes suelen venir una vez que se conocen y se saben utilizar muchas herramientas que son parte del proceso de pruebas de penetración. Las siguientes herramientas se deben conocer, instalar y probar para dar los primeros pasos en este "arte".

Kali Linux (https://www.kali.org)
Es una distribución para pruebas de penetración estándar de la industria. Es una de las distribuciones más populares entre Pentesters, Hackers éticos e investigadores de seguridad en todo el mundo y contiene cientos de herramientas para el trabajo forense, esta distribución es basada en Debian GNU/Linux.

Parrot OS (https://parrotlinux.org)
Puede verse como un laboratorio totalmente portátil para una amplia gama de operaciones de seguridad cibernética, desde pruebas de penetración hasta ingeniería inversa y análisis forense digital, pero esta distribución basada en Debian GNU/Linux también incluye todo lo que necesita para proteger sus datos y desarrollar su propio Software.

BlackArch Linux (https://blackarch.org)
Esta popular distribución de pruebas de penetración proviene de Arch Linux y contiene más de 2,400 herramientas de penetración y análisis forense diferentes, lo que le permite usar lo que necesite sin tener que descargar nuevas herramientas.

BackBox (https://www.backbox.org/)
Es una distribución de Linux basada en Ubuntu destinada a ayudar a Hackers éticos y probadores de penetración en evaluaciones de seguridad. BackBox OS está diseñado con el objetivo de ser más rápido, fácil de operar y tener un entorno de escritorio mínimo. La ventaja clave de BackBox es que sus propios repositorios de software se actualizan a intervalos regulares para mantener la distribución estable y popular para las operaciones del mundo real.

DEFT Linux (http://www.linuxandubuntu.com/home/deft-linux-a-linux-distribution-for-computer-forensics)

DEFT (Digital Evidence and Forensics Toolkit) se basa en GNU Linux y DART (Digital Advanced Response Toolkit), un sistema forense que comprende algunas de las mejores herramientas para la respuesta forense y de incidentes. DEFT Linux está especialmente diseñado para llevar a cabo tareas forenses y se ejecuta en vivo en los sistemas sin alterar el disco duro o cualquier otro medio de almacenamiento. Se compone de más de 100 herramientas forenses y de piratería de alta calificación.

Network Security Toolkit (https://www.networksecuritytoolkit.org)
El Network Security Toolkit (NST), basado en Fedora, es una versión Live que consta de las 125 principales herramientas de seguridad de código abierto proporcionadas por *insecure.org* para validar la seguridad de la red, pruebas de penetración, diagnósticos de red y monitoreo del día. El objetivo principal detrás del desarrollo de NST es proporcionar a los administradores de red/sistemas un conjunto combinado de herramientas de seguridad de código abierto para llevar a cabo operaciones como análisis de tráfico de red, detección de intrusos, escaneo de red y parches de seguridad.

Gnoppix (https://blog.desdelinux.net/gnoppix/)
Gnoppix es una distribución basada en Kali Linux Rolling diseñada para pruebas de penetración e ingeniería inversa con foco en Aplicaciones Web y obtención de acceso. Está optimizada para proteger tus derechos digitales. Pero, aunque esta centrada en la seguridad, también puede utilizarse como un escritorio normal.

6.3 Distribuciones de GNU/Linux «Inmutables»

Una distribución inmutable garantiza que el núcleo del sistema operativo permanezca sin cambios. El sistema de archivos raíz de una distribución inmutable sigue siendo de solo lectura, lo que permite permanecer igual en varias instancias. Por supuesto, puedes cambiar las cosas si así lo deseas. Sin embargo, la capacidad permanece desactivada de forma predeterminada.

¿Cómo es útil? Tradicionalmente, existían distribuciones inmutables para permitir pruebas más sencillas y desarrollo de Software basado en contenedores. Además, la inmutabilidad le brinda mayor seguridad y actualizaciones confiables para su sistema operativo. En aquel entonces, el enfoque

en dichas funciones se limitaba a las distribuciones dirigidas a profesionales y desarrolladores. Ahora se está incorporando para usuarios de escritorio diarios.

Distrobox (https://github.com/89luca89/distrobox)
esta herramienta permite instalar y ejecutar rápidamente cualquier distribución de Linux en un contenedor y garantizar su integración con el sistema principal. El proyecto proporciona un complemento sobre Docker, Podman o Lilipod, y se distingue por la máxima simplificación del trabajo y la integración del entorno de ejecución con el resto del sistema. Para crear un entorno con una distribución diferente, basta con ejecutar un solo comando distrobox-create, sin pensar en las sutilezas.

RlxOS (https://rlxos.dev/)
se enorgullece de haber sido creado desde cero como una distribución de Linux independiente para tener un mejor control sobre el núcleo y las partes funcionales. Al ser inmutable, sigue un enfoque de lanzamiento continuo para que los usuarios no necesiten reinstalarlo cada vez que haya una actualización importante. Las características clave incluyen: Inmutabilidad, Aprovecha Ostree, Se centra en la privacidad, Soporte nativo Flatpak

carbonOS (https://carbon.sh/)
carbonOS es una distribución independiente de Linux. Se centra en proporcionar una experiencia de usuario perfecta con tecnología sólida en su núcleo. Se necesita un enfoque que priorice Flatpak y contenedores. carbonOS también tiene como objetivo proporcionar actualizaciones seguras del sistema y arranque verificado como algunas características que no ofrecen todas las distribuciones atómicas. Además de sus características únicas, también quiere centrarse en brindar una excelente experiencia de escritorio GNOME.

Silverblue (https://fedoraproject.org/silverblue/)
Silverblue es una variante de Fedora Workstation con inmutabilidad. Es una de las distribuciones inmutables más populares que existen. La interfaz de usuario y la experiencia permanecen sin cambios con respecto a una versión típica de Fedora Workstation. Siempre que tenga una nueva versión de Fedora, espere también una nueva versión de Silverblue. Fedora Silverblue tiene como objetivo ofrecer una experiencia estable que sea útil

para realizar pruebas y desarrollar software basado en contenedores. Siempre puedes volver a la versión anterior del sistema operativo si algo sale mal después de una actualización.

Flatcar Container Linux (https://github.com/flatcar/Flatcar)
Flatcar es una distribución de Linux creada por la comunidad y adaptada a cargas de trabajo de contenedores, como su nombre indica. Obtiene una imagen mínima del sistema operativo que incluye solo las herramientas necesarias para ejecutar contenedores, sin administrador de paquetes y sin problemas de configuración. Si desea tener una infraestructura confiable para sus contenedores, Flatcar puede ser una buena opción que sea escalable, segura y simple al mismo tiempo. Explore más sobre esto en su página de GitHub.

NixOS (https://nixos.org/)
NixOS es una de las distribuciones de Linux más avanzadas disponibles. Pero si desea inmutabilidad y un montón de ventajas como recuperación sencilla, administrador de paquetes sólido, etc., NixOS debería ser una excelente elección. No se preocupe, si no conoce NixOS, puede explorar nuestra serie NixOS para aprender y configurarlo.

GUIX (https://guix.gnu.org/)
GUIX es similar a NixOS (más o menos) y está diseñado para usuarios avanzados que desean actualizaciones confiables y un buen control sobre sus sistemas. Si es un nuevo usuario de Linux, no debe esperar que sea su controlador diario. Por lo tanto, es posible que desees consultar su documentación para explorarla y comenzar.

openSUSE MicroOS (https://microos.opensuse.org/)
openSUSE MicroOS está diseñado para servidores donde es necesario implementar contenedores o trabajar con flujos de trabajo automatizados. Se basa en actualizaciones transaccionales que utilizan btrfs con instantáneas, lo que ayuda a guardar el historial del sistema de archivos sin ocupar mucho espacio de almacenamiento. En general, MicroOS es una opción escalable, confiable y segura para los usuarios de servidores.

Vanilla OS (https://vanillaos.org/)
Vanilla OS es un participante bastante nuevo en el espacio de la inmutabilidad. Sin embargo, logró causar sensación con su lanzamiento y luego cambió a una base Debian, abandonando Ubuntu justo después de su primer lanzamiento estable. Su objetivo es proporcionar una experiencia de escritorio fácil de usar con confiabilidad y características inmutables.

Bottlerocket (https://aws.amazon.com/bottlerocket/)
Bottlerocket es un sistema operativo de código abierto basado en Linux creado por Amazon Web Services para ejecutar contenedores en su plataforma. A diferencia de otras opciones, su uso se limita a AWS. Garantiza que los clientes que utilizan los servicios de AWS tengan una sobrecarga de mantenimiento mínima y puedan automatizar sus flujos de trabajo sin problemas. Solo puede utilizarlo como imagen de máquina de Amazon (AMI) cuando crea una Amazon Elastic Compute Cloud (EC2).

blendOS (https://blendos.co/)
blendOS es una distribución interesante en desarrollo que tiene como objetivo ofrecer todo lo bueno de otras distribuciones. En otras palabras, puede instalar cualquier paquete en la distribución (RPM, DEB, etc.) mientras obtiene la inmutabilidad y confiabilidad de actualización que cabría esperar.

Talos Linux (https://www.talos.dev/)
Talos Linux es otra distribución de Linux única, diseñada para Kubernetes. Talos Linux es una opción intrigante para los usuarios/desarrolladores de la nube. Es una opción segura, inmutable y mínima que admite plataformas en la nube, bare metal y plataformas de virtualización. También puedes iniciar fácilmente un clúster de Talos dentro de Docker. El sistema operativo se ejecuta en la memoria desde un SquashFS, lo que deja todo el disco primario a Kubernetes.

Endless OS (https://www.endlessos.org/os)
Endless OS es una distribución de Linux basada en Debian. A diferencia de cualquier otra distribución basada en Debian (por ejemplo, Ubuntu), Endless OS presenta un diseño robusto con inmutabilidad en su núcleo para garantizar que la actualización de un paquete no dañe el sistema.

6.4 Distribuciones de GNU/Linux para el «Internet de las Cosas»

Un sistema operativo de Internet de las cosas (IOT) es cualquier sistema operativo diseñado específicamente para funcionar dentro de las limitaciones particulares de los dispositivos de IoT, que generalmente están limitados en tamaño de memoria, potencia de procesamiento y capacidad, y están diseñados para permitir una transferencia rápida de datos a través de Internet.

Hay varios sistemas operativos (principalmente basados en Linux) que puedes usar para IoT, pero no te permitirán aprovechar al máximo tu configuración y esa es la razón por la que existen distribuciones centradas en IoT.

Zephyr (https://www.zephyrproject.org/)

Zephyr es un sistema operativo pequeño, escalable, de código abierto y en tiempo real (RTOS) para dispositivos conectados, que proporciona modularidad que permite a los desarrolladores optimizar el sistema para un uso específico. Admite múltiples arquitecturas y ofrece funciones como Bluetooth, LoRa y NFC. Está diseñado para ser fácil de usar y eficiente, con una pequeña huella de memoria y bajo consumo de energía. También incluye una serie de características que lo hacen adecuado para dispositivos IoT, como soporte para redes, seguridad y administración de energía.

Ubuntu Core (https://ubuntu.com/core)

Ubuntu Core es una versión robusta de la distribución más popular de Linux, Ubuntu, diseñada especialmente para grandes implementaciones de contenedores y dispositivos de Internet de las cosas. Fue creado por Canonical para utilizar el mismo kernel, Software del sistema y bibliotecas que Ubuntu, pero en una escala mucho menor, y se utiliza para alimentar robots, puertas de enlace, señales digitales, etc. Está diseñado para proporcionar a los usuarios un Linux integrado seguro para dispositivos IoT. Todos sus aspectos se verifican para mantener paquetes inmutables y firmas digitales persistentes. También es mínimo y está preparado para la empresa.

RIOT (https://www.riot-os.org/)

RIOT es un sistema operativo gratuito, amigable y de código abierto diseñado para trabajar con dispositivos IoT con el objetivo de implementar

todos los estándares abiertos relevantes que admitan conexiones IoT seguras, duraderas y respetuosas con la privacidad. Las características de RIOT incluyen un tamaño mínimo de RAM y ROM de ~1,5 kB y ~5 kB, soporte completo para C y C++, subprocesos múltiples, modularidad y MCU sin MMU.

OS Fuchsia (https://fuchsia.dev/)
OS Fuchsia es un sistema operativo en tiempo real con capacidad de código abierto creado por Google para dispositivos de Internet de las cosas. A diferencia de dos de los productos más queridos de Google, Chrome y Android, que se basan en el Kernel de Linux, Fuchsia OS se basa en el kernel Zircon. Se entrega con Node.js, que permite la compatibilidad con JavaScript y se espera que pueda ejecutarse en dispositivos AMD, así como en teléfonos y tabletas con capacidad para ejecutar aplicaciones de Android.

Embedded Linux (https://ubuntu.com/embedded)
Embedded Linux es un término utilizado para describir la última generación de sistemas operativos Linux integrados, que se basa en la distribución Ubuntu Core y presenta una serie de mejoras con respecto a versiones anteriores, que incluyen: Está diseñado para ser más liviano y eficiente, lo que lo hace ideal para dispositivos con recursos limitados, construido sobre una arquitectura modular, lo que facilita la personalización y actualización del sistema operativo, creado sobre una base segura, con funciones como AppArmor y Seccomp para proteger los dispositivos de los ciberataques, diseñado para ser nativo de la nube, lo que facilita el desarrollo, implementación y administración de aplicaciones en dispositivos integrados.

Fedora IoT (https://fedoraproject.org/iot/)
Fedora IoT es una variante del sistema operativo Fedora, diseñada para dispositivos IoT que proporciona una plataforma robusta, segura y de código abierto para la informática de punta, lo que garantiza actualizaciones constantes y un sólido apoyo de la comunidad. Con su diseño modular, Fedora IoT simplifica la administración de dispositivos, lo que lo convierte en una opción ideal para desarrolladores y empresas que se aventuran en el ecosistema de Internet de las cosas.

Windows para IoT (https://developer.microsoft.com/en-us/windows/iot/)

Windows para IoT representa el esfuerzo de Microsoft por hacerse un lugar en el floreciente panorama de Internet de las cosas (IoT). Específicamente diseñada para dispositivos IoT, esta plataforma ofrece a los desarrolladores y empresas un medio para crear soluciones inteligentes e interconectadas con un marco familiar de Windows. La plataforma se divide principalmente en dos ediciones principales, Windows 10 IoT Core y Windows 10 IoT Enterprise, y se puede integrar perfectamente con Azure IoT Suite, la solución en la nube de Microsoft para IoT, proporcionando una solución de extremo a extremo para las empresas.

6.5 Otras Distribuciones Útiles

Existe una gran variedad de distribuciones Live de Linux (The LiveCD List https://livecdlist.com/) que permiten hacer una gran cantidad de cosas útiles, a continuación damos una lista de algunas de ellas:

- KNOPPIX (http://www.knoppix.org/)
- GNOME Partition Editor (https://gparted.org/)
- System Rescue (https://www.system-rescue.org)
- Parted Magic (https://partedmagic.com/)
- Ultimate Boot (https://www.ultimatebootcd.com/)
- Super Grub2 (https://www.supergrubdisk.org/)
- Rescatux (https://www.supergrubdisk.org/rescatux/)
- Rescue (https://en.altlinux.org/Rescue)
- Ddrescue (https://www.gnu.org/software/ddrescue/)
- INSERT (http://www.inside-security.de/insert.html)
- Boot-repair (https://sourceforge.net/p/boot-repair/home/Home/)
- Rescuezilla (https://rescuezilla.com/)
- Clonezilla (https://clonezilla.org/)

- Redo Backup (ww12.redobackup.org)
- Mondo Rescue (www.mondorescue.org)
- Live Wifislax (https://www.wifislax.com/)
- Puppy Linux (http://puppylinux.com/)
- Tiny Core Linux (http://tinycorelinux.net/)
- Debian GNU/Linux Live (https://www.debian.org/CD/live/)
- Ubuntu (https://ubuntu.com/)

7 Tecnología para el Teletrabajo

Tras el impacto inicial de la pandemia provocada por el COVID-19 y, tras las medidas que probablemente se tuvieron que tomar «a toda prisa» para asegurar las operaciones de continuidad de negocio en muchas empresas, ha llegado un momento en la pregunta resuena en muchas empresas: si el teletrabajo ha llegado para quedarse, ¿Cuál es realmente la mejor forma de asegurar ese trabajo a distancia? ¿Debería invertir en más y mejores licencias VPN, o debería apostar por una solución VDI?

En términos prácticos, esta pregunta lo que significa en realidad es lo siguiente: cuando trabajan desde casa, ¿Qué tecnología debería poner a disposición de los usuarios? ¿Un escritorio virtual que les permita trabajar desde cualquier dispositivo (VDI) o un PC que les permita trabajar de forma local y que se comunique con los servidores de la compañía de forma segura (VPN)?

Ambas soluciones tienen sus pros y sus contras, por lo que en lugar de explicar cuál es mejor, lo interesante es definir qué entendemos por «mejor». Dependiendo de las distintas compañías y sus diferentes necesidades, ese «mejor» es la respuesta a preguntas como:

- ¿Cuál es más rápida de desplegar?
- ¿Cuál es la más fácil de poner en marcha?
- ¿Y la más barata?
- ¿Cuál ofrece una mejor experiencia de usuario?
- ¿Cuál se adapta mejor a lo que necesitan nuestros trabajadores?
- ¿Cuál es más segura?

Es importante tener en cuenta que ninguna de las dos opciones ofrece un «Sí» rotundo a todas las preguntas a la vez, por lo que hay que tener en cuenta cuáles son nuestras prioridades. Pero es que además, deberíamos ser capaces de responder a algunas preguntas adicionales como:

- ¿A qué aplicaciones tenemos que dar soporte? ¿Son Web-apps, aplicaciones para Windows, otras...?

- ¿Trabajamos solo con aplicaciones on-premises, o trabajamos también con aplicaciones Cloud y SaaS?
- ¿Tenemos experiencia con entornos VDI? ¿Tendríamos que empezar desde cero, o contamos con un entorno previo?
- ¿Tenemos experiencia gestionando dispositivos corporativos fuera del perímetro de seguridad de nuestra organización?
- Y los empleados...¿Disponen ya de portátiles con los que trabajar desde casa o deberían hacerse con equipos nuevos? (Y si no los tienen, ¿los va a proveer la empresa o va a incentivar su compra?)
- ¿Cómo gestiona la empresa sus dispositivos en estos momentos? ¿Cuenta con una solución Cloud moderna para hacerlo?
- ¿Dispone ya de licencias VPN? ¿Dispone de licencias suficientes para dar soporte a la plantilla completa? ¿Tiene un ancho de banda suficiente para todos ellos? Y si no lo tiene... ¿Hay medidas sencillas que se pueden poner en marcha para liberar espacio?
- ¿Cómo se relacionan con estas soluciones los otros componentes de la infraestructura tecnológica? (Ej: el acceso a archivos «Legacy» funciona mejor a través de VDI, mientras que el trabajo con soluciones como DropBox o OneDrive es más sencillo con un escritorio no virtualizado).
- ¿Existe en la organización, sector, algún tipo de regulación o Compliance que incline necesariamente la balanza hacia una u otra solución?

Al responder todas estas preguntas, no sería extraño acabar por determinar que lo más interesante es trabajar con un escenario mixto: uno en el que el caso de uso para algunos usuarios estuviera muy claro en favor de VPN, mientras que para otros lo más interesante fuera apostar por VDI, o viceversa.

7.1 VDI en el Teletrabajo: Ventajas e Inconvenientes

Un infraestructura de VDI es un conjunto de tecnologías que lo que hacen es virtualizar los escritorios de los empleados de una empresa, alojándolos

normalmente en su propio centro de datos. De esta forma, normalmente utilizando un navegador Web, los trabajadores pueden acceder al mismo escritorio que están acostumbrados a utilizar en su empresa (información, aplicaciones, correo corporativo, etc.) desde cualquier dispositivo. Las ventajas de trabajar de esta forma, son evidentes:

- No importa con qué equipo se cuente en casa (un portátil de alta gama, una vieja torre de sobremesa, una tablet...). Basta una conexión a internet, una pantalla y un teclado para que la experiencia siempre sea idéntica.
- Conectarse a un escritorio VDI no exige ningún tipo de habilidad especial por parte del usuario. Si son capaces de recordar su nombre de usuario y su contraseña, pueden empezar a trabajar en su ordenador corporativo en pocos segundos.
- Un escritorio virtualizado es altamente seguro, ya que tanto las aplicaciones como los datos con los que trabaja el usuario se encuentran bien en los servidores de la compañía, bien en el Cloud.

Que estas ventajas sean desde luego importantes y atractivas para muchas empresas, no quiere decir sin embargo que no haya ciertos inconvenientes a tener en cuenta, siendo los principales:

- Poner en marcha una infraestructura VDI puede ser complejo. Si no disponemos de una estructura previa, el proceso inicial puede ser costoso y se necesitan expertos IT que nos asesoren en todo el proceso.
- Todos los teletrabajadores deben contar en su domicilio una conexión a internet de calidad. Una interrupción en el servicio implicará que no puedan hacer nada.
- VDI requiere más ancho de banda y potencia en los servidores, sobre todo a la hora de trabajar con grandes o múltiples pantallas. Si en el centro de datos de la empresa se producen «cuellos de botella», la experiencia de usuario se resiente.
- No todas las aplicaciones ofrecen una experiencia óptima en VDI y curiosamente, las de audio o video conferencia son las que peor experiencia ofrecen (de hecho, muchos Managers tienden a pedir que estas aplicaciones se ejecuten fuera de este entorno).

- VDI supone en la práctica «pagar» por un portátil para cada usuario... alojado en el servidor de la empresa...por lo que si esos usuarios ya disponen de equipos corporativos validados, tal vez estemos pagando dos veces por los mismos equipos.

7.2 VPN en el Teletrabajo: Ventajas e Inconvenientes

Como muchos saben, una conexión VPN es ese «túnel» virtual que conecta los equipos de los trabajadores de una empresa con el centro de datos de la misma, cuando estos se encuentran en una oficina distante o, como en esta situación, se encuentran teletrabajando. Esto facilita que los usuarios utilicen equipos corporativos en su hogar, de forma local, a la vez que se securizan sus comunicaciones. Lo cual tiene muchas ventajas como que:

- Si los usuarios ya disponen de un «portátil de empresa», no tienen que hacer nada. Pueden seguir trabajando de la misma forma que lo harían en la oficina.
- Es una opción más barata que el VDI. No hace falta invertir en servidores dedicados o invertir en licencias VDI Cloud que son bastante más caras.

Pero como en el caso de los escritorios virtuales, trabajar con conexiones VPN también tiene aspectos «no tan bonitos» a tener en cuenta como:

- Como las aplicaciones corporativas se encuentran en los ordenadores de cada uno de los usuarios, se incrementan y se dificultan las tareas de mantenimiento.
- También hay que considerar el mantenimiento de los propios equipos o su reemplazo, en el caso de que se queden obsoletos.
- El usuario va a tener total libertad para poder trabajar con la información corporativa de su empresa de forma local...lo cual desde el punto de vista de la seguridad no es lo ideal.
- Una VPN pone el dispositivo del usuario en la red de la empresa, lo que implica que todos los parches de seguridad, las actualizaciones de las aplicaciones y del sistema operativo, la distribución de software en general... se realiza a través de este tipo de conectividad. ¿Podemos asegurar que estas tareas se están realizando con regularidad?

- Para los usuarios que no dispongan de un equipo corporativo, puede ser todo un desafío replicar la configuración de los mismos, en uno que acaban de comprar, sin pasar antes por el departamento TI de la empresa.

- Si necesitamos adquirir nuevos equipos para los trabajadores, ¿estamos seguros que nuestra imagen de Windows va a funcionar exactamente igual que en los equipos «antiguos»? ¿Pueden darse problemas de compatibilidad? ¿Cuánto tiempo puede llevar realizar una instalación «remota» de todo lo que necesitan?

- La mayoría de los programas de VPN realizan comprobaciones de seguridad antes de permitir que el usuario se conecte a la VPN. Por ejemplo, estas comprobaciones pueden asegurar que el dispositivo está actualizado con parches, antivirus, etc. Si todo el mundo que trabaja desde casa ralentiza el proceso de actualización y aplicación de parches, ¿podremos rebajar el estándar de seguridad para permitir que las máquinas más retrasadas entren en la VPN?

Lo cierto sin embargo es que en el caso de la VPN, algunas de las desventajas solo se presentan si lo que estamos utilizando es una plataforma tradicional, como puede ser Microsoft SCCM, GPOs, VPN on-prem... y en gran medida desaparecen si apostamos en cambio por plataformas de gestión (VMware Workspace ONE, etc.), que aprovechan las capacidades Cloud de Windows 10 que permiten a los usuarios inscribir automáticamente sus dispositivos en la red de la empresa, y que automatizan desde la nube todas las tareas de actualización de aplicaciones, seguridad y mantenimiento.

Pero incluso así, no hay una respuesta sencilla. Finalmente el departamento de TI debe apostar por aquella en la que crea que pueden sentirse más cómodos, lo que, en grandes equipos de trabajo pasará en muchas ocasiones (e insistimos en esto), en una combinación de ambas opciones.

8 Seguridad y Privacidad en el Software

Tal como se observa en los principios que guían este trabajo, garantizar la seguridad, la confiabilidad, la resiliencia y la estabilidad de las aplicaciones y servicios de internet es fundamental para fomentar la confianza en su uso. Como usuarios de dispositivos interconectados en internet, debemos tener un alto grado de confianza en que internet, sus aplicaciones y los dispositivos conectados a la red son lo suficientemente seguros como para realizar en línea toda la gama de actividades que deseamos en relación con la tolerancia al riesgo asociado con tales actividades.

En este sentido, el uso de internet desde nuestros dispositivos que esta proliferando actualmente no es diferente y está fundamentalmente relacionada con la capacidad de los usuarios de confiar en su entorno. Si los usuarios no creen que los dispositivos que tienen conectados y su información están razonablemente seguros contra el mal uso o los daños, la erosión de la confianza resultante provoca una renuencia a usar internet.

Esto tiene consecuencias globales para el comercio electrónico, la innovación técnica, la libertad de expresión y prácticamente para todos los demás aspectos de las actividades en línea. En efecto, para garantizar la seguridad en los productos y servicios basados en internet, el sector desarrollador de productos digitales debe considerar la seguridad como una de sus máximas prioridades. A medida que conectamos cada vez más dispositivos a internet, surgen nuevas oportunidades para explotar vulnerabilidades potenciales de seguridad.

Los dispositivos mal asegurados pueden servir como puntos de entrada para ciberataques, permitiendo que personas malintencionadas puedan reprogramar un dispositivo o perjudicar su funcionamiento. Los dispositivos mal diseñados pueden exponer los datos de los usuarios a robos, dejando los flujos de usuarios sin una protección adecuada. Los dispositivos defectuosos o que no funcionan bien también pueden crear vulnerabilidades.

Estos problemas son tanto o más graves en el caso de los dispositivos inteligentes pequeños, baratos y ubicuos en internet. Los desafíos que imponen la competitividad de los costos y las limitaciones técnicas hacen que para los fabricantes de estos dispositivos no sea fácil diseñar funciones de seguridad adecuadas, potencialmente generando, a largo plazo, vulnerabi-lidades en la seguridad y dificultades en el mantenimiento superiores a las computadoras tradicionales.

Junto con posibles deficiencias en el diseño de la seguridad, el enorme au-

mento del número y la variedad de los dispositivos conectados a la red podría aumentar las oportunidades de ataque. Sumado a la naturaleza altamente interconectada de los dispositivos inteligentes, cada dispositivo mal asegurado conectado en línea potencialmente afecta la seguridad y la resistencia de internet a nivel global, no solo a nivel local. Por ejemplo, un refrigerador o un televisor sin protección infectado con Malware que se encuentra en Estados Unidos pueden enviar miles de correos electrónicos no deseados dañinos a destinatarios de todo el mundo usando la conexión Wi-Fi de la casa.

Para complicar todavía más las cosas, en un mundo hiperconectado, nuestra capacidad de funcionar diariamente sin dispositivos o sistemas conectados a internet probablemente disminuirá. De hecho, es cada vez más difícil comprar ciertos dispositivos sin conexión a internet, ya que algunos fabricantes solo ofrecen productos conectados. Cada vez estamos más conectados y dependemos más de los dispositivos para muchos servicios esenciales, por lo que necesitamos que los dispositivos sean seguros.

Pero también reconocemos que ningún dispositivo puede ser absolutamente seguro. Este creciente nivel de dependencia de los dispositivos y de los servicios de internet con los cuales interactúan también aumentan las formas que tienen los delincuentes para acceder a los dispositivos interconectados a la red. Si se ven comprometidas en un ataque cibernético, quizá podríamos desenchufar nuestros televisores conectados a internet, pero no es tan fácil apagar un medidor inteligente de energía eléctrica, un sistema de control de tráfico o un marcapasos si estos dispositivos son víctimas de un ataque malicioso. Esta es la razón por la cual la seguridad de los dispositivos y servicios debe ser un importante punto de discusión y un tema crítico por atender. Dependemos cada vez más de estos dispositivos para servicios esenciales, por lo que su comportamiento puede tener un alcance y un impacto globales.

8.1 Consideraciones de Seguridad

Al pensar en los dispositivos conectados a internet, es importante entender que la seguridad de estos dispositivos no es absoluta. La seguridad de los dispositivos no es una proposición binaria de tipo seguro/inseguro. Por el contrario, resulta útil conceptualizar la seguridad de los dispositivos como un espectro de vulnerabilidad. El espectro va desde dispositivos totalmente desprotegidos sin ninguna función de seguridad hasta sistemas muy seguros con múltiples capas de elementos de seguridad.

En un constante juego de gato y ratón, a medida que las nuevas amenazas de seguridad evolucionan, los fabricantes de dispositivos y los operadores de redes responden para hacer frente a las nuevas amenazas. La seguridad general y la resiliencia de los dispositivos interconectados al internet dependen de cómo se evalúen y gestionen los riesgos de seguridad.

La seguridad de un dispositivo está en función del riesgo en que un dispositivo se vea comprometido, del daño que tal compromiso provocaría, tiempo y los recursos necesarios para lograr cierto nivel de protección. Si un usuario no puede tolerar un alto grado de riesgo (por ejemplo, un operador de un sistema de control de tráfico o una persona a quien se le ha implantado un dispositivo médico que está conectado a internet), puede que para dicho usuario sienta que se justifica gastar una cantidad considerable de recursos para proteger el sistema o el dispositivo contra un ataque.

Del mismo modo, si una persona no le preocupa que su refrigerador pueda ser Hackeado y utilizado para enviar Spam, puede que no se sienta obligada a pagar por un modelo que tenga un diseño de seguridad más sofisticado si esto hace que el dispositivo sea más costoso o complicado. En esta evaluación y cálculo de la mitigación de los riesgos influyen diferentes factores. Estos factores incluyen una comprensión clara de los riesgos de seguridad actuales y posibles riesgos futuros, la estimación de los costos económicos y otros tipos de daños si los riesgos se hacen realidad y el costo estimado de la mitigación de estos.

Si bien este tipo de concesiones de seguridad muchas veces se realizan desde la perspectiva de los usuarios individuales y las organizaciones, también es importante tener en cuenta la interrelación de los dispositivos interconectados como parte de un ecosistema mayor. La conectividad en red de los dispositivos significa que las decisiones de seguridad que se toman a nivel local con respecto a un dispositivo pueden tener impactos globales sobre otros dispositivos.

Como cuestión de principio, quienes desarrollan objetos inteligentes para internet tienen la obligación de garantizar que estos dispositivos no expongan los bienes de sus propios usuarios ni de otras personas a potenciales daños. Como cuestión de negocios y de economía, los fabricantes desean reducir sus costos, su complejidad y su tiempo de comercialización. Por ejemplo, son cada vez más comunes los dispositivos de alto volumen y bajo margen de ganancia y que ya representan un costo adicional para los productos en los que están embebidos; añadir más memoria y un procesador más rápido para implementar medidas de seguridad podría hacer que el producto ya no fuera

competitivo.

En términos económicos, el resultado de la falta de seguridad en los dispositivos digitales es una externalidad negativa, donde una o más partes imponen un costo sobre otras. Un ejemplo clásico es la contaminación del medio ambiente, donde los costos de los daños y la limpieza (externalidades negativas) resultantes de las acciones de quien contamina son asumidos por otras partes. El hecho es que el costo de la externalidad impuesto a los demás normalmente no se considera en el proceso de toma de decisiones, a menos que, como es el caso de la contaminación, se aplique un impuesto que sirva de aliciente para reducir la contaminación.

De acuerdo con Bruce Schneier, en el caso de la seguridad de la información surge una externalidad cuando el proveedor que crea el producto no corre con los costos que ocasionan las potenciales inseguridades; en este caso, una ley de responsabilidad puede convencer a los vendedores para que tomen en cuenta la externalidad y desarrollen productos más seguros. Estas consideraciones de seguridad no son nuevas en el contexto de la tecnología, pero la magnitud de los desafíos que pueden surgir en las implementaciones de dispositivos digitales de gran volumen las vuelve extremadamente significativas. Estos desafíos se describen a continuación.

Desafíos de Seguridad que son Exclusivos de los Dispositivos Interconectados. Las diferencias entre los dispositivos digitales, las computadoras y los dispositivos informáticos tradicionales suelen desafiar la seguridad:

- Muchos dispositivos digitales interconectados (por ejemplo, los sensores y los artículos de consumo) están diseñados para ser desplegados a una escala masiva que es varios órdenes de magnitud superior a la de los dispositivos tradicionalmente conectados a internet. Por consiguiente, la cantidad potencial de enlaces interconectados entre estos dispositivos no tiene precedentes. Además, muchos de estos dispositivos podrán establecer enlaces y comunicarse con otros dispositivos por sí mismos, de manera impredecible y dinámica. Por lo tanto, puede ser necesario considerar nuevamente las herramientas, métodos y estrategias existentes asociadas con la seguridad de los dispositivos.

- Muchos despliegues de dispositivos consistirán en colecciones de dispositivos idénticos o prácticamente idénticos. Esta homogeneidad amplifica el potencial impacto de cualquier vulnerabilidad de seguridad

simplemente por la gran cantidad de dispositivos que tienen las mismas características. Por ejemplo, una vulnerabilidad en el protocolo de comunicación de una marca de bombillas de luz conectadas a internet se podría extender a todas las marcas y modelos de dispositivos que utilizan el mismo protocolo o que comparten características clave de diseño o fabricación.

- Muchos de los dispositivos digitales que se van a desplegar tendrán una vida útil anticipada superior a la que típicamente se espera para los equipos de alta tecnología. Además, estos dispositivos se podrían desplegar en circunstancias que los harían difíciles o imposibles de reconfigurar o actualizar; o bien estos dispositivos podrían sobrevivir a la empresa que los creó, lo que los dejaría huérfanos y sin apoyo a largo plazo. Estos escenarios ilustran que los mecanismos de seguridad que son adecuados en el momento del despliegue podrían no ser adecuados durante toda la vida útil del dispositivo y a medida que las amenazas a la seguridad evolucionen, esta situación podría crear vulnerabilidades que persistirían por mucho tiempo. Esto contrasta con el paradigma de los sistemas de computadoras tradicionales en los cuales normalmente se aplican actualizaciones al sistema operativo durante toda la vida de servicio de los equipos para hacer frente a las amenazas de seguridad. El apoyo y la gestión a largo plazo de los dispositivos digitales interconectados representa un importante reto de seguridad.

- Muchos dispositivos digitales están diseñados intencionadamente sin ninguna posibilidad de actualización; en otros, el proceso de actualización es engorroso o poco práctico. Por ejemplo, consideremos el retiro de 1.4 millones de automóviles Fiat Chrysler 2015 para arreglar una vulnerabilidad que potencialmente permitiría Hackear el vehículo en forma inalámbrica. Estos vehículos se deben llevar a un concesionario Fiat Chrysler para que les realicen una actualización manual del Software, o bien los propietarios deben actualizar el Software por sí mismos usando una memoria USB. La realidad es que un alto porcentaje de estos automóviles probablemente no se actualizarán porque el proceso de actualización representa un inconveniente para los propietarios, esto los deja permanentemente vulnerables a las amenazas de seguridad cibernética, sobre todo porque el automóvil parece estar funcionando muy bien.

- Muchos dispositivos digitales funcionan de modo que es escasa o nula la visibilidad que tiene el usuario de su funcionamiento interno o de los flujos de datos que producen. Si un usuario cree que un dispositivo está ejecutando ciertas funciones pero en realidad está ejecutando funciones no deseadas o recogiendo más información que lo que el usuario desea, se crea una vulnerabilidad. Las funciones del dispositivo también podrían cambiar sin previo aviso cuando el fabricante ofrece una actualización, lo que deja al usuario vulnerable a cualquier cambio que este realice.

- Algunos dispositivos digitales probablemente serán desplegados en lugares donde sea difícil o imposible lograr la seguridad física. Los atacantes pueden tener acceso físico directo a los dispositivos. Para garantizar la seguridad será necesario considerar el uso de protección contra manipulaciones y otras innovaciones de diseño.

- Al igual que muchos sensores ambientales, algunos dispositivos digitales han sido diseñados para ser integrados discretamente en su entorno, donde los usuarios apenas se den cuenta de su presencia o monitoreen su funcionamiento. Además, los dispositivos pueden no tener una forma clara de alertar al usuario cuando surge un problema de seguridad, por lo que es difícil para un usuario saber que la seguridad de un dispositivo digital ha sido vulnerada. Esta situación podría persistir por mucho tiempo antes de ser detectada y corregida; incluso podría darse el caso de que no fuera posible o práctico implementar una corrección o mitigación. Del mismo modo, el usuario podría no ser consciente de que existe un sensor en su entorno, por lo que potencialmente un fallo de seguridad podría persistir por mucho tiempo sin ser detectado.

- Los primeros modelos digitales serán producto de grandes empresas de tecnología privadas y/o públicas. Sin embargo, en el futuro "construir su propia internet de las cosas" (Build Your Own Internet Of Things) podría convertirse en algo habitual, como lo demuestra el crecimiento de las comunidades de desarrolladores de Arduino y Raspberry Pi. Estos despliegues podrán o no aplicar los estándares de mejores prácticas de seguridad de la industria.

Preguntas Relacionadas con la Seguridad de los Dispositivos Interconectados Se han planteado una serie de preguntas con respecto a

los problemas de seguridad que plantea el uso de dispositivos digitales interconectados. Muchas de estas preguntas ya existían antes del crecimiento explosivo de los dispositivos interconectados, pero su importancia ha aumentado debido a la magnitud del despliegue de los dispositivos utilizados. A continuación veremos las preguntas más importantes:

Buenas Prácticas de Diseño ¿Cuáles son las mejores prácticas que los ingenieros y desarrolladores deben utilizar al diseñar dispositivos digitales para que sean más seguros?, ¿cómo se recogen y transmiten las lecciones aprendidas a partir de los problemas de seguridad de los dispositivos a las comunidades de desarrolladores para mejorar las futuras generaciones de dispositivos?, ¿qué formación y recursos educativos se pueden utilizar para enseñar a los ingenieros y desarrolladores para diseñar una gama de dispositivos más segura?.

Equilibrio Entre Costo y Seguridad ¿De qué manera las partes interesadas toman decisiones informadas con respecto a los dispositivos digitales interconectados considerando la relación costo-beneficio?, ¿cómo se pueden cuantificar y evaluar con precisión los riesgos de seguridad?, ¿qué motivará a los diseñadores y fabricantes de dispositivos para que acepten el costo adicional que implica el diseño de dispositivos más seguros, en particular, para que asuman la responsabilidad por el impacto de cualquier externalidad negativa derivada de sus decisiones de seguridad?, ¿cómo se van a conciliar las incompatibilidades entre la funcionalidad, la facilidad de uso y la seguridad?, ¿cómo nos aseguramos de que las soluciones de seguridad para los dispositivos digitales interconectados soporten oportunidades para la innovación y de crecimiento económico?.

Estándares e Indicadores ¿Qué papel desempeñan los estándares técnicos y operativos en el desarrollo y despliegue de dispositivos digitales interconectados seguros y de buen funcionamiento?, ¿cómo se pueden identificar y medir las características de seguridad de los dispositivos digitales interconectados?, ¿cómo se puede medir la efectividad de las iniciativas y medidas de seguridad implementadas?, ¿cómo se puede asegurar la implementación de mejores prácticas de seguridad?.

Confidencialidad de los Datos, Autentificación y Control de Acceso ¿Cuál es el papel óptimo del cifrado de los datos con respecto a los dispositivos digitales?, ¿utilizar tecnologías de cifrado, autenticación y control de acceso en los dispositivos digitales es una solución adecuada para evitar intentos de espionaje y secuestro de los flujos de datos que producen estos dispositivos?, ¿qué tecnologías de cifrado y autenticación se podrían adaptar para los dispositivos digitales y cómo se podrían aplicar considerando las limitaciones de costo, tamaño y velocidad de procesamiento de los dispositivos?, ¿cuáles son los problemas de gestión que se espera deberán ser abordados como resultado del cifrado a una escala de la magnitud de los dispositivos digitales interconectados?, ¿se están abordando las preocupaciones con respecto a cómo gestionar el ciclo de vida de las claves criptográficas y el período durante el cual se espera que un algoritmo dado permanezca seguro?, ¿los procesos de extremo a extremo son lo suficientemente seguros y simples como para que los utilicen los usuarios típicos?.

Capacidad de Actualización en Campo Dado que se espera que muchos de los dispositivos digitales tendrán una vida útil prolongada, ¿estos dispositivos deben diseñarse considerando su mantenimiento y su capacidad de actualización in situ de modo que puedan adaptarse a las nuevas amenazas de seguridad?. Si cada dispositivo tiene integrado un agente de gestión de dispositivos, en los dispositivos digitales interconectados se podría instalar y configurar nuevo Software. Pero los sistemas de gestión aumentan los costos y la complejidad, ¿habrá otros enfoques para actualizar el Software de los dispositivos que sean más compatibles con el uso masivo de los dispositivos digitales?, ¿existe alguna clase de dispositivos de bajo riesgo y que por lo tanto no justifique este tipo de características?. En general, ¿las interfaces de usuario de los dispositivos interconectados (por lo general mínimas) se están analizando adecuadamente, tomando en cuenta la gestión de los dispositivos (por parte de cualquier persona, incluso por el usuario)?.

Responsabilidad Compartida ¿Cómo se puede fomentar la responsabilidad compartida y la colaboración entre todas las partes interesadas en pos de la seguridad de los dispositivos digitales interconectados.

Regulación ¿Se debe sancionar a los fabricantes de dispositivos por la venta de Software o Hardware con fallos de seguridad conocidas o descono-

cidas?, ¿cómo se podrían adaptar o ampliar las leyes de responsabilidad de producto y protección del consumidor para que abarquen las externalidades negativas relacionadas con los dispositivos digitales interconectados?, ¿sería posible hacerlo en un entorno transfronterizo?, ¿la regulación podrá seguir el ritmo y mantener su eficacia en vista de la evolución de la tecnología de los dispositivos y la evolución de las amenazas a la seguridad?, ¿cómo se debe equilibrar la regulación con las necesidades de la innovación sin pedir permiso, la libertad en internet y la libertad de expresión?.

Obsolescencia de los Dispositivos ¿Qué enfoque se debe adoptar con respecto a los dispositivos digitales obsoletos a medida que internet evoluciona y cambian las amenazas a la seguridad?, ¿se debe exigir que los dispositivos tengan una funcionalidad de "final de vida" integrada que los inactive?. En el futuro, este tipo de requisito podría obligar a sacar de servicio a los dispositivos más antiguos que no son interoperables y a reemplazarlos por dispositivos más seguros e interoperables. Esto ciertamente sería muy difícil en un mercado abierto. ¿Qué implicaciones tiene la inactivación automática de los dispositivos digitales interconectados?.

La amplitud de estas preguntas es representativo de la variedad de las consideraciones de seguridad asociadas con los dispositivos digitales interconectados. Sin embargo, es importante recordar que, cuando un dispositivo está en internet también es parte de internet, lo que significa que solo se pueden lograr soluciones de seguridad eficaces y apropiadas si todas las partes involucradas con estos dispositivos aplican un enfoque de seguridad colaborativo.

Tanto entre la industria como entre los gobiernos y las autoridades públicas, el modelo colaborativo aparece como un enfoque eficaz para ayudar a asegurar a internet y al ciberespacio. Este modelo incluye una serie de prácticas y herramientas que incluyen el intercambio de información bidireccional y voluntario, herramientas de aplicación eficaces, preparación para incidentes y ejercicios cibernéticos, creación de conciencia y capacitación, acuerdo sobre las normas de comportamiento internacionales, desarrollo y reconocimiento de prácticas y estándares internacionales.

Es necesario continuar trabajando para que sigan evolucionando los enfoques colaborativos y basados en la gestión de riesgos, a manera de lograr que se adapten bien a la escala y la complejidad de los desafíos de seguridad de los dispositivos digitales interconectados.

8.2 Consideraciones Sobre la Privacidad

El respeto por las expectativas y los derechos de privacidad es fundamental para asegurar la confianza en internet; además, también afecta la capacidad de las personas de hablar, conectarse y escoger de formas significativas. Estos derechos y expectativas se suelen enmarcar en términos del manejo ético de los datos, que hacen hincapié en la importancia de respetar las expectativas de privacidad del individuo y el uso legítimo de sus datos. El uso de dispositivos digitales masivo puede desafiar estas expectativas tradicionales de privacidad. El uso masivo de dispositivos digitales suele referirse a una amplia red de dispositivos con sensores diseñados para recopilar datos acerca de su entorno, que muchas veces incluyen datos relacionados con las personas.

Estos datos presumiblemente proporcionan un beneficio al propietario del dispositivo, pero muchas veces también benefician al fabricante o proveedor. La recopilación y el uso de los datos se convierte en una consideración de privacidad cuando las expectativas de privacidad de quienes son observados por los dispositivos digitales difieren de las de quienes recogerán y usarán estos datos. También hay combinaciones de flujos de datos aparentemente inocentes que también pueden poner en riesgo la privacidad.

Cuando se combinan o correlacionan flujos de datos individuales, el retrato digital que se obtiene de las personas suele ser más invasivo que el que se puede obtener a partir de un flujo de datos individual. Por ejemplo, un cepillo de dientes con conexión a internet puede recoger y transmitir información sobre los hábitos de cepillado de una persona, algo bastante inocuo. En cambio, si el refrigerador de este mismo usuario informa el listado de los alimentos que consume y si además el dispositivo que el usuario utiliza para llevar cuenta de su actividad física también informa los datos correspondientes, la combinación de estos flujos de datos pinta una descripción mucho más detallada y privada de la salud general de la persona.

Este efecto de agregación de los datos puede ser particularmente potente en el caso de los dispositivos digitales interconectados, dado que muchos producen otros metadatos como por ejemplo marcas de tiempo e información de geolocalización, lo que aumenta aún más la especificidad del usuario. En otras situaciones, el usuario puede no ser consciente de que un dispositivo está recogiendo datos sobre su persona y potencialmente compartiéndolos con terceros. Este tipo de recolección de datos es cada vez más frecuente en los dispositivos de consumo, como por ejemplo en los televisores inteligentes y las consolas de videojuegos. Este tipo de productos tienen características

de reconocimiento de voz o de visualización que permanentemente escuchan las conversaciones u observan la actividad en una habitación y selectivamente transmiten los datos recogidos a un servicio en la nube para su procesamiento, donde a veces participa un tercero.

Una persona podría estar en presencia de este tipo de dispositivos sin saber que sus conversaciones o actividades están siendo monitoreadas o que sus datos están siendo registrados. Estos tipos de características pueden ser de beneficio para un usuario informado, pero pueden plantear un problema de privacidad para quienes no son conscientes de la presencia de estos dispositivos y no pueden influir significativamente sobre la forma en que se utiliza la información recogida.

Sin importar si el usuario está al tanto de que los dispositivos digitales recogen y analizan sus datos, estas situaciones ponen de relieve el valor que tienen estos flujos de datos personalizados para empresas y organizaciones que buscan recoger y sacar provecho de la información obtenida a través de los dispositivos digitales interconectados a internet. La demanda de esta información deja al descubierto los desafíos legales y regulatorios que enfrentan las leyes de protección de datos y privacidad.

Es fundamental abordar estos tipos de problemas de privacidad, dado que tienen implicaciones sobre nuestros derechos básicos y nuestra capacidad colectiva de confiar en internet. Desde una perspectiva más amplia, las personas reconocen que su privacidad es un valor intrínseco y tienen expectativas con respecto a los datos personales que se pueden recoger y cómo estos datos pueden ser utilizados por terceros. Esta noción general acerca de la privacidad también vale para los datos recogidos por los dispositivos digitales interconectados a internet, pero estos dispositivos pueden socavar la capacidad del usuario de expresar y hacer cumplir sus preferencias de privacidad. Si el hecho de que sus preferencias de privacidad no sean respetadas por los dispositivos digitales, hace que los usuarios pierdan la confianza en internet, entonces podría disminuir el mayor valor que este tiene.

En general, la forma en que los dispositivos digitales interconectados aumentan la viabilidad y el alcance de la vigilancia y el seguimiento amplifica las preocupaciones relativas a la privacidad. Las características de los dispositivos digitales interconectados y las formas en que se utilizan redefinen el debate sobre los temas de privacidad, ya que modifican drásticamente cómo se recogen, analizan, utilizan y protegen los datos personales. Por ejemplo:

- El modelo tradicional de privacidad de "notificación y consentimiento"

en que los usuarios hacen valer sus preferencias de privacidad interactuando directamente con información que aparece en la pantalla de una computadora o dispositivo móvil (por ejemplo, haciendo clic en "Acepto") deja de funcionar cuando los sistemas no le ofrecen al usuario ningún mecanismo de interacción. Muchas veces los dispositivos digitales no tienen una interfaz de usuario para configurar las preferencias de privacidad y en muchas configuraciones los usuarios no tienen conocimiento ni controlan la forma en que se recogen y utilizan sus datos personales. Esto provoca una brecha entre las preferencias de privacidad del usuario y el comportamiento de recolección de datos del dispositivo. Si consideran que los datos recopilados no son datos personales, es posible que los proveedores de dispositivos se sientan menos incentivados a ofrecer a los usuarios un mecanismo para que expresen sus preferencias de privacidad. Sin embargo, la experiencia demuestra que, en realidad, los datos que tradicionalmente no se consideran personales podrían ser o convertirse en datos personales si se combinan con otros.

- Suponiendo que se pudiera desarrollar un mecanismo eficaz que permitiera que un usuario expresara de manera informada sus preferencias de privacidad, este mecanismo debería poder manejar la gran cantidad de dispositivos digitales interconectados que debe controlar cada usuario. No es realista pensar que un usuario interactuará directamente con cada uno de los dispositivos con que se encuentre a lo largo del día para expresar sus preferencias de privacidad. Por el contrario, las interfaces de privacidad se deben poder escalar de acuerdo con el tamaño del problema, sin dejar de ser completas y prácticas desde la perspectiva del usuario.

- Los dispositivos digitales interconectados pueden poner en peligro las expectativas de los usuarios con respecto a la privacidad en situaciones comunes. Las normas sociales y expectativas de privacidad difieren en los espacios públicos frente a los espacios privados; los dispositivos digitales interconectados desafían estas normas. Por ejemplo, las tecnologías de vigilancia que utiliza cámaras de vigilancia o los sistemas de trazabilidad de ubicación que normalmente funcionan en espacios públicos están migrando hacia espacios tradicionalmente privados como el hogar o los vehículos particulares, donde nuestras expectativas de

privacidad son muy diferentes. Al hacerlo, desafían lo que muchas sociedades reconocen como el derecho a la privacidad en el hogar o los espacios privados. Además, las expectativas de las personas con respecto a su privacidad en los espacios que consideran públicos (parques, centros comerciales, estaciones de tren, etc.) también están siendo desafiadas por el aumento de la naturaleza y el alcance de la vigilancia en tales espacios.

- Muchas veces los dispositivos digitales interconectados funcionan en contextos donde la proximidad expone a múltiples personas a una misma actividad de recolección de datos. Por ejemplo, el sensor de seguimiento por geolocalización de un automóvil podría registrar los datos de localización de todos los ocupantes del vehículo, sin importar si estas personas desean que lo haga o no. Incluso podría realizar un seguimiento de las personas que viajan en otros vehículos cercanos. En este tipo de situaciones podría ser difícil o imposible distinguir -mucho menos respetar- las preferencias de privacidad individuales.

- El análisis de datos personales consolidados a gran escala de por sí representa un riesgo sustancial de invasión a la privacidad y potencial discriminación. Este riesgo se amplifica en los dispositivos digitales interconectados debido a la escala y a la mayor intimidad de la recolección de datos personales. Los dispositivos digitales interconectados pueden recoger información personal con un grado de especificidad y penetración sin precedente; agregar y correlacionar estos datos permite crear perfiles personales detallados que pueden generar un riesgo potencial para la discriminación y otros daños. La sofisticación de esta tecnología puede crear situaciones que expongan al individuo a daños físicos, penales, financieros o de reputación.

- La ubicuidad, familiaridad y aceptación social de muchos dispositivos digitales interconectados pueden crear una falsa sensación de seguridad y alentar a las personas a divulgar información confidencial o privada sin pleno conocimiento o apreciación de las posibles consecuencias.

Preguntas Relacionadas con la Privacidad de los Dispositivos interconectados Estas preguntas referidas a la privacidad serían un desafío incluso si estuvieran bien alineados los intereses y motivaciones de todas las

partes involucradas en el ecosistema de los dispositivos digitales interconectados. Sin embargo, sabemos que las relaciones y los intereses de quienes están expuestos a la recolección de sus datos personales y quienes agregan, analizan y utilizan los datos pueden ser desequilibrados o injustos.

La fuente de datos puede ver una intrusión no deseada a su espacio privado, muchas veces sin consentimiento, control, elección o incluso conciencia. No obstante, quien recoge los datos podría considerarlos un recurso beneficioso que puede añadir valor a sus productos y servicios y proporcionar nuevas fuentes de ingresos. Dado que los dispositivos digitales interconectados desafían nuestras nociones de privacidad de formas nunca antes vistas, al reevaluar los modelos de privacidad en línea en el contexto de los dispositivos digitales interconectados, es necesario responder ciertas preguntas clave. Algunas de las preguntas que se han planteado incluyen las siguientes:

Legitimidad en la Recopilación y el Uso de los Datos en el contexto de los dispositivos digitales interconectados, ¿cómo se resuelve la relación de mercado entre las fuentes de los datos y quiénes los recogen?. Los datos personales tienen un valor personal y comercial diferente según se consideren desde el punto de vista de las fuentes o de los recolectores, tanto indivi-dualmente como en su conjunto; por lo tanto, ambas partes tienen intereses legítimos que podrían estar en conflicto. ¿Cómo se pueden expresar estos diferentes intereses de una manera que conduzca a reglas en materia de acceso, control, transparencia y protección que sean justas y consistentes, tanto para las fuentes como para los recolectores?.

Transparencia, Expresión y Cumplimiento de las Preferencias de Privacidad ¿cómo se puede hacer que las políticas y prácticas de privacidad sean de fácil acceso y comprensibles en el contexto de los dispositivos digitales interconectados?, ¿cuáles son las alternativas al modelo tradicional de privacidad de "notificación y consentimiento" que podrían abordar los aspectos únicos de los dispositivos digitales interconectados?, ¿cuál sería un modelo eficaz para expresar, aplicar y hacer cumplir las preferencias de privacidad individuales y las preferencias multipartitas?, ¿se podría construir un modelo multipartito de este tipo?. De ser así, ¿qué aspecto tendría?, ¿cómo se podría aplicar a circunstancias concretas que impliquen las preferencias de privacidad individuales?, ¿existe un mercado para tercerizar la gestión de la configuración de la privacidad a servicios comerciales diseñados para

implementar las preferencias de los usuarios?, ¿es necesario que exista un Proxy de privacidad que exprese y haga cumplir las preferencias del usuario a través de una serie de dispositivos, al tiempo que elimine la necesidad de interacción directa con cada uno de ellos?.

Gran variedad de Expectativas de Privacidad las normas y expectativas de privacidad están estrechamente relacionadas con el contexto social y cultural del usuario, que puede variar de una nación o de un grupo a otro. Muchos escenarios de los dispositivos digitales interconectados implican el despliegue de dispositivos y actividades de recopilación de datos de alcance multinacional o global que atraviesan fronteras sociales y culturales. ¿Qué implicará esto para el desarrollo de un modelo de protección de la privacidad que se pueda aplicar ampliamente a los dispositivos digitales interconectados?, ¿cómo se pueden adaptar los dispositivos y sistemas de dispositivos digitales interconectados para que reconozcan y respeten la variedad de expectativas de privacidad de los usuarios y las diferentes legislaciones?.

Privacidad por Diseño ¿cómo se pueden adaptar los dispositivos y sistemas digitales para que reconozcan y respeten la variedad de expectativas de privacidad de los usuarios y las diferentes legislaciones?, ¿cómo se puede animar a los fabricantes de dispositivos digitales interconectables para que incorporen los principios de la privacidad por diseño a sus valores fundamentales?, ¿cómo se puede fomentar la inclusión de consideraciones sobre la privacidad de los consumidores en todas las fases de desarrollo y operación de los productos?, ¿cómo se pueden conciliar los requisitos de funcionalidad y privacidad?. En principio, los fabricantes deberían anticipar que, a largo plazo, los productos y las prácticas que respeten la privacidad se ganarán la confianza y la satisfacción de los clientes y generarán lealtad hacia la marca. ¿Es esta motivación suficiente para competir con los deseos de simplicidad en el diseño y velocidad en el mercado?, ¿los dispositivos se deberían diseñar con una configuración predeterminada para el modo de recopilación de datos más conservador (es decir, no recopilación de datos por defecto)?.

Identificación ¿cómo debemos proteger los datos recogidos por los dispositivos digitales interconectados que parecieran no ser personales donde se recogen o que han sido "desidentificados", pero que en algún momento futuro podrían llegar a ser datos personales (por ejemplo, porque podrían ser

re-identificados o combinados con otros datos).

El uso de dispositivos digitales interconectados genera desafíos únicos para la privacidad que van más allá de los problemas que existen en la actualidad. Es necesario desarrollar estrategias para respetar las opciones de privacidad individuales considerando un amplio espectro de expectativas, sin dejar de fomentar la innovación en nuevas tecnologías para los dispositivos digitales.

8.3 Software Libre e Infraestructura Crítica

Si bien, el ecosistema de Software libre es una de las empresas más grandiosa en la historia de la humanidad, en los últimos tiempos los gobiernos, industrias de todos los sectores económicos y personal académico se ha visto en la apremiante necesidad de comprender el Software más importante que corre en las infraestructuras críticas de todos los ámbitos de nuestra vida, si bien existe una gran cantidad de Software libre, algunos han llegado a ser el pilar de nuestra vida tecnológica.

El Software libre se ejecuta en una gran cantidad de dispositivos (desde teléfonos inteligentes, tabletas, computadoras, dispositivos de interconexión de red, etc.) del planeta y mantiene en funcionamiento la infraestructura crítica de gran parte del mundo. Es por ello que agencias de todo el mundo (entre ellas DARPA), están preocupadas por cuanto se puede confiar en dicho Software.

No es una gran exageración decir que gran parte de la infraestructura del mundo está construida sobre Software libre y en particular sobre el Kernel de Linux, aunque la mayoría de la gente nunca ha oído hablar de él. Es uno de los primeros programas que se cargan cuando la mayoría de los dispositivos de cómputo en cuanto se encienden. Permite que el Hardware que ejecuta la máquina interactúe con el Software, gobierna el uso de recursos y actúa como la base del sistema operativo.

Es el bloque de construcción central de casi toda la computación en la nube, prácticamente todas las supercomputadoras, todo el Internet de las cosas, miles de millones de teléfonos inteligentes y más.

Pero el Kernel también es de código abierto, lo que significa que cualquiera puede escribir, leer y usar su código. Y eso tiene a los expertos en seguridad cibernética del mundo seriamente preocupados. Su naturaleza de código abierto significa que el Kernel de Linux, junto con una gran cantidad de otras

piezas de Software crítico de código abierto, está expuesto a una manipulación hostil en formas que apenas entendemos.

La gente apenas se está dando cuenta ahora que literalmente gran parte de lo que hacemos está respaldado por Linux. Esta es una tecnología fundamental para nuestra sociedad, no comprender la seguridad del Kernel significa que no se podrá asegurar la infraestructura crítica.

De los proyectos que han salido a la luz pública, la agencia gubernamental DARPA (el brazo de investigación del ejército de EE. UU.) quiere comprender la colisión de código y comunidad que hace que estos proyectos de código abierto funcionen, para comprender mejor los riesgos que enfrentan. El objetivo es poder reconocer de manera efectiva a los actores maliciosos y evitar que interrumpan o corrompan el código de código abierto de importancia crucial antes de que sea demasiado tarde.

Por ejemplo, el programa "Social Cyber" de DARPA es un proyecto multimillonario de 18 meses de duración que combinará la sociología con los avances tecnológicos recientes en inteligencia artificial para mapear, comprender y proteger estas comunidades masivas de código abierto y el código que crean. Es diferente de la mayoría de las investigaciones anteriores porque combina el análisis automatizado tanto del código como de las dimensiones sociales del Software de código abierto.

Amenazas al Software Libre Gran parte de la civilización moderna ahora depende de un corpus de código abierto en constante expansión porque ahorra dinero, atrae talento y facilita mucho el trabajo. Pero si bien el movimiento de código abierto ha generado un ecosistema colosal del que todos dependemos, no lo entendemos completamente, argumentan expertos. Hay innumerables proyectos de Software, millones de líneas de código, numerosas listas de correo, foros y un océano de colaboradores cuyas identidades y motivaciones a menudo son oscuras, lo que dificulta responsabilizarlos.

Eso puede ser peligroso. Por ejemplo, los piratas informáticos han insertado discretamente códigos maliciosos en proyectos de código abierto en numerosas ocasiones en los últimos años. Las puertas traseras pueden escapar durante mucho tiempo a la detección y en el peor de los casos, se han entregado proyectos completos a malos actores que se aprovechan de la confianza que las personas depositan en las comunidades y el código de código abierto.

A veces hay interrupciones o incluso tomas de control de las mismas redes

sociales de las que dependen estos proyectos. El seguimiento de todo ha sido principalmente, aunque no del todo, un esfuerzo manual, lo que significa que no coincide con el tamaño astronómico del problema.

Varios autores argumentan que necesitamos el aprendizaje automático para digerir y comprender el universo en expansión del código, lo que significa trucos útiles como el descubrimiento automatizado de vulnerabilidades, así como herramientas para comprender la comunidad de personas que escriben, corrigen, implementan e influyen en ese código.

El objetivo final es detectar y contrarrestar cualquier campaña maliciosa para enviar código defectuoso, lanzar operaciones de influencia, sabotear el desarrollo o incluso tomar el control de proyectos de código abierto.

Para hacer esto, los investigadores utilizarán herramientas como el análisis de sentimientos para analizar las interacciones sociales dentro de las comunidades de código abierto, como la lista de correo del Kernel de Linux, que debería ayudar a identificar quién es positivo o constructivo y quién es negativo y destructivo.

Los investigadores quieren conocer qué tipos de eventos y comportamientos pueden perturbar o dañar las comunidades de código abierto, qué miembros son confiables y si hay grupos particulares que justifiquen una vigilancia adicional. Estas respuestas son necesariamente subjetivas. Pero en este momento hay pocas formas de encontrarlos.

A los expertos les preocupa que los puntos ciegos de las personas que ejecutan el Software de código abierto hagan que todo el edificio esté listo para posibles manipulaciones y ataques. Para algunos investigadores, la principal amenaza es la perspectiva de un "código no confiable" que ejecute la infraestructura crítica del mundo, una situación que podría generar sorpresas desagradables.

Preguntas Sin Respuesta Así es como funciona el programa "Social Cyber": DARPA ha contratado a varios equipos de lo que llama "intérpretes", incluidos pequeños talleres de investigación de ciberseguridad boutique con habilidades técnicas profundas.

Uno de estos actores es Margin Research, con sede en Nueva York, que ha reunido a un equipo de investigadores muy respetados para la tarea. Él ha dicho que existe una necesidad desesperada de tratar a las comunidades y proyectos de código abierto con un mayor nivel de cuidado y respeto, ya que mucha de la infraestructura existente es muy frágil porque depende del código

abierto, que asumimos que siempre estará ahí porque siempre ha estado ahí. Esto es alejarse de la confianza implícita que tenemos en las bases de código y Software de fuente abierta.

Muchos investigadores se han enfocado en el Kernel de Linux en parte porque es tan grande y crítico que tener éxito aquí, a esta escala, significa que puede hacerlo en cualquier otro lugar. El plan es analizar tanto el código como la comunidad para visualizar y finalmente comprender todo el ecosistema.

El trabajo de los investigadores mapea quién está trabajando en qué partes específicas de los proyectos de código abierto. Por ejemplo, Huawei es actualmente el mayor contribuyente al Kernel de Linux. Otro colaborador trabaja para Positive Technologies, una empresa rusa de ciberseguridad que, al igual que Huawei, ha sido sancionada por el gobierno de EE. UU. También se ha mapeado código escrito por empleados de la NSA, muchos de los cuales participan en diferentes proyectos de código abierto.

Este tipo de investigación también tiene como objetivo encontrar la inversión insuficiente, es decir, Software crítico ejecutado en su totalidad por uno o dos voluntarios. Es más común de lo que podría pensar, tan común que una forma común en que los proyectos de Software actualmente miden el riesgo es el "factor del autobús": ¿Todo este proyecto se desmorona si solo una persona es atropellada por un autobús?

Si bien la importancia del Kernel de Linux para los sistemas informáticos del mundo puede ser el problema más apremiante para "Social Cyber", también abordará otros proyectos de código abierto. Ciertos artistas se centrarán en proyectos como Python, un lenguaje de programación de código abierto utilizado en una gran cantidad de proyectos de inteligencia artificial y aprendizaje automático.

La esperanza es que una mayor comprensión facilite la prevención de un desastre futuro, ya sea que sea causado por una actividad maliciosa o no. Prácticamente dondequiera que mires, encuentras Software de código abierto, incluso cuando miras el Software propietario, un estudio reciente mostró que en realidad es 70% o más de código abierto.

Este es un problema de infraestructura crítica y no se tiene el control sobre eso. Y una gran cantidad de investigadores cree que se debe controlar. El impacto potencial es que los Hackers malintencionados siempre tendrán acceso a las máquinas Linux. Eso incluye a los teléfonos. Es así de simple.

Google Ofrece su Software de Código Abierto para Preservar la Seguridad La seguridad informática y el Software de código abierto continúan siendo una gran preocupación para los desarrolladores y las organizaciones. En este sentido, un estudio realizado en 2022 por Synopsys alertó sobre la inquietud que producía la ciberseguridad, y donde se señalaba que el 84% de las bases de código de Software de código abierto contenían alguna vulnerabilidad conocida, un dato que suponía un aumento del 4% respecto al año 2021.

En vista a esto, en el pasado mes de mayo de 2022, Google anunció la salida de su nuevo servicio Assured Open Source Software (OSS asegurado), un servicio de Software de código abierto que permitiría a las empresas defenderse de los ataques a la seguridad. El gerente de soluciones de Software de Synopsys, Mike McGuire, explicó el especial interés que tiene Google en que la comunidad de código abierto sea lo más segura posible.

El lanzamiento de Assured OSS ha venido motivado por la creciente cantidad de ataques cibernéticos dirigidos a proveedores de código abierto, según admitió el gerente de productos, seguridad y privacidad de Google, Andy Chang. Por entonces, se informó de un aumento del 650% de estos ataques a la cadena de suministro de Google ofrece su Software de código abierto para preservar la seguridad. Chang dijo por entonces que "Google está en una posición única para ayudar en esta área, ya que somos colaboradores, mantenedores y usuarios de Software de código abierto desde hace mucho tiempo, y hemos desarrollado un sólido conjunto de tecnología, procesos, capacidades de seguridad y controles".

El proceso, anuncia ahora la compañía especializada en productos y servicios relacionados con internet, Software, dispositivos electrónicos y otras tecnologías, se realizaría escaneando y analizando de forma periódica algunas bibliotecas de Software más conocidas a nivel mundial, en busca de vulnerabilidades.

El lanzamiento de Google es una realidad, y Assured OSS se pone a disponibilidad de los usuarios del sector público y empresarial de forma gratuita, permitiendo que éstos incorporen los mismos paquetes de Software de código abierto que emplea Google.

Assured OSS en Respuesta a las Amenazas Ocultas El servicio Assured Open Source Software llega para los ecosistemas Java y Pynthon gratis, después de que durante mucho tiempo dependiera de bibliotecas a

terceros y tras conocer realmente el carácter de las amenazas cuando la Casa Blanca se vio afectada. Tras este hecho, Google se tomó muy en serio el asunto de la ciberseguridad en la cadena de suministro de Software.

En su comunicado oficial, Google ha asegurado que mantendrá de forma constante las bibliotecas actualizadas buscando ventanas abiertas de vulnerabilidad y detectando nuevas que puedan desarrollarse. Una vez identificado algún peligro, ejecutará sus correcciones para dar solución al peligro en el menor tiempo posible. De esta manera, la analista de ESG Melinda Marks, afirmó categóricamente que "a medida que las organizaciones utilizan cada vez más OSS para ciclos de desarrollo más rápidos, necesitan fuentes confiables de paquetes seguros de código abierto".

Además Marks añadió que "sin la investigación y verificación adecuadas o los metadatos para ayudar a rastrear el acceso y el uso de OSS, las organizaciones corren el riesgo de exponerse a posibles vulnerabilidades de seguridad y otros riesgos en su cadena de suministro de Software. Al asociarse con un proveedor confiable, las organizaciones pueden mitigar estos riesgos y garantizar la integridad de su cadena de suministro de Software para proteger mejor sus aplicaciones comerciales".

Para poder tener acceso a este nuevo servicio, Google ha informado al respecto, que los desarrolladores y las organizaciones sólo deberán registrarse y posteriormente integrar Assured OSS en su proceso de desarrollo. Con este sencillo proceso tendrán toda la seguridad que proporciona el nuevo paquete de la compañía.

La OpenELA (Open Enterprise Linux Association), una asociación formada el año 2023 por CIQ (Rocky Linux), Oracle y SUSE se ha unido para garantizar la compatibilidad con RHEL (Red Hat Enterprise Linux). Dentro de este marco, han presentado el proyecto Kernel-lts, el cual proporcionará soporte adicional para algunas ramas obsoletas de Kernels LTS después de que dejen de recibir soporte oficial.

Con el lanzamiento de este proyecto, la versión 4.14, será la primera rama del Kernel que recibirá este soporte adicional (esta versión del Kernel fue lanzada en noviembre de 2017 y ha recibido soporte durante 6 años). En enero 2024, el equipo de desarrollo del Kernel dejó de mantener esta rama y OpenELA ha asumido el mantenimiento y las actualizaciones para el Kernel 4.14 se lanzarán al menos hasta diciembre de 2024. Tras la última versión del Kernel de Linux 4.14.336, el equipo de OpenELA ha lanzado

las actualizaciones extendidas 4.14.337-openela, 4.14.338-openela y 4.14.339-openela.

El mantenimiento proporcionado por OpenELA seguirá las mismas reglas y procesos que se aplican a los Kernels LTS estables normales. No habrá restricciones adicionales, como la vinculación a equipos o productos específicos. Las actualizaciones se publicarán basadas en el trabajo de seguimiento de correcciones en las ramas actuales del kernel y su migración a las ramas LTS extendidas mantenidas por OpenELA.

Además, la Fundación Linux proporciona ramas SLTS (Super Long Term Support) basadas en los Kernels 4.4, 4.19, 5.10 y 6.1. Estas ramas SLTS se mantienen por separado y reciben soporte durante períodos extendidos de 10 a 20 años. El proyecto Civil Infrastructure Platform (CIP) es responsable de mantener estas ramas SLTS, con la participación de empresas como Toshiba, Siemens, Renesas, Bosch, Hitachi, MOXA, mantenedores de las ramas LTS del núcleo principal, desarrolladores de Debian y el proyecto KernelCI. Estas ramas SLTS están diseñadas para su aplicación en sistemas técnicos de infraestructura civil y en sistemas industriales críticos.

9 Búsquedas en Deep y Dark Web

Los internautas cada vez tienen más curiosidad por la Deep y Dark Web que no está indexada en los motores habituales de búsqueda como Google, Yahoo! o Bing. Según estiman los expertos, esta parte oculta podría tener un tamaño muy superior al de Internet que utilizamos todos los días. Así, se calcula que la Deep Web ocupa en torno al 90% del contenido de la World Wide Web. Si queremos acceder a toda esta información también podemos usar unos buscadores propios que son distintos a los tradicionales. En esta sección hablaremos de cómo internarse en la Deep Web con estos buscadores que nos facilitarán la navegación por ella.

Lo primero que vamos a hacer es conocer los diferentes tipos de Web y por qué existen. Luego veremos si con cualquier tipo de navegador podemos acceder a ella y cómo podemos entrar. Después podremos ver como acceder a la Deep Web con buscadores especializados y que podemos encontrar en ella.

9.1 ¿Qué es Web Superficial, la Deep y Dark Web?

La Internet tiene un tamaño considerable, con millones de páginas Web, bases de datos y servidores que funcionan las 24 horas del día. Pero el denominado Internet "visible" (sitios que se pueden encontrar a través de motores de búsqueda, como Google y Yahoo) solo es la punta del iceberg.

Hay una serie de términos relacionados con la red no visible, pero vale la pena saber diferenciarlos si tiene empleado explorar una ruta de navegación alternativa.

La Web Superficial o la Web Abierta es la capa superficial "visible". Si continuamos visualizando toda la Web como un iceberg, la Web abierta sería la parte superior que está sobre el agua. Desde un punto de vista estadístico, este conjunto de sitios Web y datos constituye menos del 5 % del total de Internet.

Aquí se encuentran todos los sitios Web disponibles al público a los que se accede a través de los navegadores tradicionales como Google Chrome, Internet Explorer y Firefox. Los sitios Web se suelen identificar con operadores de registro como ".com" y ".org" y pueden localizarse fácilmente con los motores de búsqueda más populares.

La localización de sitios Web superficiales es posible porque los motores de búsqueda pueden indexar la Web a través de enlaces visibles (un proceso llamado "rastreo" debido a que el motor de búsqueda recorre la Web como una araña).

La Deep y Dark Web el concepto de Deep Web se atribuye al informático Mike Bergman y hace referencia al contenido de Internet que no está indexado por los motores de búsqueda convencionales, como por ejemplo Google, debido a diversos factores. La principal causa por la que existe la Deep Web es porque hay información que no se quiere que esté indexada por los principales motores de búsqueda como Google, Yahoo! o Bing, por este motivo, tenemos buscadores específicos donde sí están indexada esta información dentro de la red Tor.

La Deep Web se encuentra debajo de la superficie y representa aproximadamente el 90 % de todos los sitios Web. Esta sería la parte de un iceberg debajo del agua, mucho más grande que la Web superficial. De hecho, esta Web oculta es tan grande que es imposible determinar con exactitud cuántas páginas o sitios Web están activos en un momento dado.

Siguiendo con la analogía, los grandes motores de búsqueda podrían considerarse como barcos de pesca que solo pueden "atrapar" sitios Web cerca de la superficie. Todo lo demás, desde revistas académicas hasta bases de datos privadas y más contenido ilícito, está fuera de alcance. Esta Web profunda también incluye la parte que conocemos como la Web oscura o Dark Web.

Si bien muchos medios de comunicación utilizan indistintamente la "Web profunda o Deep Web " y la "Web oscura o Dark Web", gran parte de la parte profunda en su conjunto es perfectamente legal y segura. Algunas de las partes más grandes de la Web profunda incluyen:

- Bases de datos: colecciones de archivos tanto públicas como privadas protegidas que no están conectadas a otras áreas de la Web, solo para que se busquen dentro de la propia base de datos.
- Intranets: redes internas de empresas, gobiernos e instalaciones educativas utilizadas para comunicar y controlar aspectos privados dentro de sus organizaciones.

La Deep Web se utiliza para mantener la actividad de internet privada y en el anonimato, lo que puede ser útil tanto en aplicaciones legales como

ilegales. Si bien algunos la utilizan para evadir la censura del gobierno, también se sabe que se utiliza para actividades altamente ilegales.

9.2 Acceso a la Deep Web

En caso de que se esté preguntando cómo acceder a la Web profunda, es probable que ya la esté utilizando a diario. El término "Web profunda" hace referencia a todas las páginas Web que los motores de búsqueda no pueden identificar. Los sitios de la Web profunda pueden esconderse detrás de contraseñas u otros muros de seguridad, mientras que otros simplemente le dicen a los motores de búsqueda que no los "rastreen". Sin enlaces visibles, estas páginas están más ocultas por varias razones.

En la Web profunda más grande, su contenido "oculto" es generalmente más limpio y seguro. Todo, desde las publicaciones de blogs en revisión y rediseños de páginas Web pendientes, hasta las páginas a las que accede cuando realiza una transacción bancaria en línea, forma parte de la Web profunda. Además, no suponen ninguna amenaza para su equipo ni para la seguridad en general. Por ejemplo, el área privada de una empresa, la zona de usuario de una operadora o la Web privada de una universidad, tienen información que no está indexada en ningún buscador. Sin embargo, todo el mundo atribuye el término Deep Web a cosas ilegales y lo cierto es que todo contenido sin indexar entra en la categoría.

La mayoría de estas páginas se mantienen ocultas de la Web abierta para proteger la información y la privacidad del usuario, como por ejemplo:

- Cuentas financieras como banca y planes de jubilación
- Cuentas de correo electrónico y mensajería de redes sociales
- Bases de datos de empresas privadas
- La información confidencial de la documentación médica
- Archivos legales

Adentrarse más en la Web profunda trae un poco más de peligro a la luz. Para algunos usuarios, partes de la red profunda ofrecen la oportunidad de pasar por alto las restricciones locales y acceder a servicios de televisión o películas que pueden no estar disponibles en sus áreas locales. Otros la

utilizan para descargar música pirateada o hacerse con películas que todavía no están en el cine.

En el extremo oscuro de la Web, encontrará el contenido y la actividad más peligrosos. Los sitios Web Tor se encuentran en este extremo de la Web profunda, que se consideran la "Web oscura" y solamente se puede acceder a ellos utilizando un navegador anónimo.

La seguridad en la Web profunda es más relevante para el usuario medio de Internet que la seguridad en la Web oscura, ya que podría terminar en zonas peligrosas por accidente: todavía se puede acceder a muchas partes de la Web profunda con navegadores de Internet normales. Así es como los usuarios pueden navegar a través de suficientes vías tangenciales y terminar en un sitio de piratería, un foro políticamente radical o viendo contenidos inquietantemente violentos.

9.3 Acceso a la Dark Web

La Web oscura o Dark Web se refiere a los sitios que no están indexados y a los que solo se puede acceder a través de nave-gadores Web especializados. Significativamente más pequeña que la diminuta Web superficial, la Web oscura se considera parte de la Web profunda. Al usar nuestro océano y un iceberg como referencia, la Web oscura sería la punta inferior del iceberg sumergido.

La Web oscura, sin embargo, es una parte muy oculta de la Web profunda con la que pocos interactúan o incluso visitan. En otras palabras, la red profunda abarca todo lo que hay bajo la superficie y sigue siendo accesible con el Software adecuado, incluida la red oscura.

El análisis de la construcción de la Web oscura revela algunas capas clave que la convierten en un refugio anónimo:

- No hay indexación de páginas Web por parte de los motores de búsqueda de la Web superficial. Google y otras herramientas de búsqueda populares no pueden descubrir o mostrar resultados de páginas dentro de la Web oscura.
- "Túneles de tráfico virtual" a través de una infraestructura de red aleatoria.
- Inaccesible para los navegadores tradicionales debido a su único operador de registro. Además, está oculta por varias medidas de seguridad

de la red como los cortafuegos y el cifrado.

La reputación de la Web oscura se ha vinculado a menudo a la intención criminal o al contenido ilegal, y a sitios de "comercio" en los que los usuarios pueden adquirir bienes o servicios ilícitos. Sin embargo, las partes legales también han hecho uso de esta plataforma.

Cuando se trata de la seguridad de la Web oscura, los peligros de la Web profunda son muy diferentes de los peligros de la Web oscura. La actividad cibernética ilegal no tiene por qué ser fácil de encontrar, pero tiende a ser mucho más extrema y amenazadora si se busca.

Para muchos la red Tor es la base de la Deep Web y Dark Web, en el mundo de Tor todo el tráfico está cifrado y anonimizado, porque pasamos por diferentes nodos entre un origen y un destino, de hecho, podríamos acceder a la Web normal a través de la red Tor para anonimizar lo máximo posible todo el tráfico de red. Por supuesto, cuando alguien levanta una Web en la red Tor, la única forma de acceder a ella es con enlaces directos, no hay indexación, aunque sí tenemos algunos «buscadores» que disponen de una gran cantidad de direcciones de Tor para acceder directamente a estos servicios.

Es conocido por muchos que Tor es una de las Darknets, pero lo cierto es que existen otras como Freenet o I2P con recursos muy valiosos. Se puede decir que la red oscura es una colección de redes y tecnologías usadas para compartir información y contenidos digitales. Estas utilizan protocolos y puertos «no estándares» sobre la red subyacente. La definición varía según los autores, ya que otros creen que deben también ocultar la identidad misma de los miembros de la red.

Se puede dar como ejemplo de redes Darknet las redes Freenet, i2p, GNUnet, Entropy, ANts P2P, y Tor, por lo que no debemos quedarnos únicamente con Tor como máximo exponente de la Deep Web o Dark Web. Tenemos dos tipos, las de tipo P2P o Peer-to-Peer como Freenet, i2p, GNUnet, Entropy, ANts P2P y las no P2P como Tor. Las primeras destacan por su anonimato frente a las segundas.

¿Puedo Acceder a la Deep Web a Través de Google? aunque la gran mayoría de nosotros utilizamos buscadores como Google, Bing o Yahoo!, tal y como hemos explicado antes, la información que se encuentra en Tor no está indexada en estos motores de búsqueda y por lo tanto será necesario recurrir a otros para acceder a las páginas Web que se encuentran en esta parte de internet. Por tanto, no vas a poder acceder a la Deep Web a través de los

buscadores «normales», sino que tendrás que utilizar buscadores específicos para navegar por todo el contenido que hay por al Deep Web.

Lo que sí podríamos buscar en Google y en otros buscadores son los navegadores o sistemas operativos específicos para entrar en la Deep Web, como el popular Tor Browser que es ampliamente utilizado para navegar fácilmente por Tor sin necesidad de realizar un reenvío de todo el tráfico de Internet, algo que no sería muy recomendable hacer.

¿Puedo Usar el Navegador Web de Siempre? En principio sí, pero deberás instalar un programa para reenviar todo el tráfico de tu ordenador a través de la red Tor, de esta forma, sí podrías usar un navegador normal como Firefox o Google Chrome, sin embargo, lo más recomendable es utilizar un navegador Web específico para navegar por la red Tor, como el navegador Tor Browser que está basado en Firefox.

Con este navegador Web no tendrás que instalar ningún tipo de programa adicional, simplemente tendremos que instalar el navegador Tor Browser y empezaremos a navegar por la red Tor sin necesidad de ningún Software adicional.

El navegador de red Tor (proyecto "The Onion Routing") proporciona a los usuarios acceso para visitar sitios Web con el operador de registro ".onion". Este navegador es un servicio desarrollado originalmente a finales de la década de 1990 por el Laboratorio de Investigación Naval de los Estados Unidos.

Al comprender que la naturaleza de Internet significaba una falta de privacidad, se creó una versión temprana de Tor para ocultar las comunicaciones de espías. Con el tiempo, la plataforma se redefinió y desde entonces se ha hecho pública en la forma del navegador que conocemos hoy en día. Cualquiera puede descargarlo gratuitamente.

Piense en Tor como en un navegador Web como Google Chrome o Firefox. Sin embargo, en lugar de seleccionar la ruta más directa entre su ordenador y las partes profundas de la Web, el navegador Tor utiliza una ruta aleatoria de servidores cifrados conocidos como "nodos". Esto permite a los usuarios conectarse a la Web profunda sin temor a que sus acciones se rastreen o a que su historial de navegación se exponga.

Los sitios en la Web profunda también utilizan Tor (o un Software similar, como I2P, el "Proyecto de Internet Invisible") para mantener su anonimato, es decir, que no es posible averiguar quién los administra ni dónde se alojan.

¿Es Ilegal Entrar en la Web Oscura? en pocas palabras, no es ilegal acceder a la Web oscura. De hecho, algunos usos son perfectamente legales y apoyan el valor de la "Web oscura". En la Web oscura, los usuarios pueden buscar tres beneficios claros de su uso:

- Anonimato del usuario
- Servicios y sitios prácticamente imposibles de rastrear
- Capacidad de adoptar medidas ilegales tanto para los usuarios como para los proveedores

De este modo, la Web oscura ha atraído a muchas partes que, de otro modo, estarían en peligro al revelar sus identidades en línea. Las víctimas de abusos y persecuciones, los informantes y los disidentes políticos han sido usuarios frecuentes de estos sitios ocultos. Pero, por supuesto, esos beneficios pueden extenderse fácilmente a quienes deseen actuar fuera de las limitaciones de las leyes de otras formas explícitamente ilegales.

Cuando se ve a través de esta lente, la legalidad de la Web oscura se basa en la forma en que usted, como usuario, se involucra con ella. Puede rozar el límite de la legalidad por muchas razones que son importantes para la protección de la libertad. Otros pueden actuar de manera ilegal para la protección y la seguridad de los demás. Explicaremos ambos conceptos en términos de "navegador de la Web oscura" y los propios sitios Web.

¿Es Ilegal Utilizar Tor? por lo que respecta al Software, el uso de Tor y otros navegadores anonimizados no es estrictamente ilegal. De hecho, estos supuestos navegadores de la "Web oscura" no están vinculados exclusivamente a esta parte de Internet. Muchos usuarios utilizan ahora el navegador Tor para navegar tanto en la Internet pública como en las partes más profundas de la Web de forma privada.

La privacidad que ofrece el navegador Tor es importante en la era digital actual. En la actualidad, tanto las empresas como los órganos rectores participan en la vigilancia no autorizada de la actividad en línea. Algunos simplemente no quieren que las agencias gubernamentales o incluso los proveedores de servicios de Internet (ISP) sepan lo que están viendo en línea, mientras que otros tienen pocas opciones. A menudo se impide a los usuarios de países con leyes estrictas de acceso y de usuario acceder incluso a sitios públicos, a menos que utilicen clientes de Tor y redes privadas virtuales (VPN).

Sin embargo, todavía se pueden tomar acciones ilegales dentro de Tor que podrían incriminar al usuario sin importar la legalidad del navegador. Podría utilizar Tor en un intento de piratear contenido con derechos de autor de la Web profunda, compartir pornografía ilegal o participar en ciberterrorismo. El uso de un navegador legal no hará que tus acciones estén en el lado correcto de la ley.

¿Es Ilegal Utilizar y Visitar los Sitios de la Web Oscura? en el extremo de la red, la Web oscura es un poco más como una zona gris. Utilizar la Web oscura suele significar que se está intentando realizar una actividad que, de otro modo, no podría llevarse a cabo a la vista del público.

Para los críticos del gobierno y otros defensores francos, pueden temer una reacción negativa si se descubren sus verdaderas identidades. En el caso de aquellos que han sufrido daño a manos de otros, pueden no querer que sus atacantes descubran sus conversaciones sobre el evento. Si una actividad es considerada ilegal por los órganos rectores a los que pertenece, entonces sería ilegal.

Por supuesto, el anonimato tiene una parte negativa, ya que los criminales y los Hackers maliciosos también prefieren operar en la clandestinidad. Por ejemplo, los ciberataques y el tráfico son actividades por las cuales los participantes saben que serán incriminados. Por esto motivo llevan estas acciones a la Web oscura, para ocultarse.

En última instancia, el simple hecho de navegar por estos espacios no es ilegal, pero puede ser un problema para el usuario. Aunque no es ilegal en su totalidad, cierto es que se llevan a cabo actividades desagradables en muchas partes de la Web oscura. Puede exponerle a riesgos innecesarios si no es cuidadoso/a o no tiene conocimientos avanzados, es experto/a en informática y consciente de sus amenazas. Entonces, ¿para qué se utiliza la Web oscura cuando se usa para actividades ilegales?

¿Me Pueden Espiar en la Deep Web? el apogeo de buscar contenido y almacenarlos en esta parte de Internet está provocado por los casos de espionaje que se han descubierto en los últimos años. Sobre todo el de la NSA marcó un punto de inflexión, pero a día de hoy son muchas las compañías que están señaladas por espiar a los usuarios o recopilar datos de forma ilegítima, a pesar de la declaración de privacidad existente en el servicio.

En principio, solamente los nodos de entrada y salida de la red Tor podrían

conseguir la información en texto plano y espiar a los usuarios, no obstante, en el caso de que utilicemos una capa extra de seguridad como una VPN, esto no sería posible realizarlo porque la información ya va cifrada internamente en el túnel. Aunque se ha conocido de casos en que entidades gubernamentales han obtenido datos de usuarios aún en estos túneles cifrados.

9.4 Tipos de Amenazas en la Web Oscura

Si está considerando utilizar la Web oscura con fines de privacidad básica, podría preguntarse: "¿Es peligroso usar la Web oscura?" Desafortunadamente, puede ser un lugar peligroso. A continuación se presentan algunas amenazas comunes a las que puede enfrentarse durante sus experiencias de navegación:

Software Malicioso es decir, el Malware, está presente y completamente activo en toda la Web oscura. A menudo se ofrece en algunos portales para dar a los actores de amenazas las herramientas para llevar a cabo los ciberataques. Sin embargo, también persiste en toda la Web oscura para infectar a usuarios desprevenidos como lo hace en el resto de la Web.

La Web oscura no tiene tantos contratos sociales como los que siguen los proveedores de sitios Web para proteger a los usuarios del resto de la Web. Por lo tanto, los usuarios pueden verse expuestos regularmente a algunos tipos de malware como:

- Keyloggers
- Malware de Botnet
- Ransomware
- Malware de Phishing

Si decide seguir explorando cualquier sitio de la Web oscura, se pone en riesgo de que le señalen y se convierta en blanco de los Hackers y más. Los programas de protección de Endpoints pueden detectar la mayoría de las infecciones de Malware.

Las amenazas de la navegación en línea pueden extenderse al mundo desconectado si pueden explotar su equipo o su conexión de red. El anonimato es fuerte con Tor y la plataforma de la Web oscura, pero no es infalible. Cualquier actividad en línea puede dejar rastros hasta su identidad si alguien investiga lo suficiente.

Supervisión del gobierno con muchos sitios basados en Tor investigados por las autoridades policiales en todo el mundo, existe un claro peligro de convertirse en objetivo del gobierno por el simple hecho de visitar un sitio Web oscuro.

Los mercados de drogas ilegales como la Ruta de la seda han sido secuestradas para vigilancia policial en el pasado. Utilizar Software personalizado para infiltrarse y analizar la actividad ha permitido a los funcionarios descubrir las identidades de los usuarios, tanto de los visitantes como de los transeúntes. Incluso si nunca ha realizado ninguna compra, es posible que le vigilen e incriminen por otras actividades en un momento posterior.

Las infiltraciones pueden ponerle en riesgo de que le vigilen también por otro tipo de actividades. Evadir las restricciones gubernamentales para explorar nuevas ideologías políticas puede ser un delito con pena de prisión en algunos países. China utiliza lo que se conoce como el "Gran cortafuegos" que limita el acceso a los sitios populares por esta misma razón. El riesgo de ser un visitante de este contenido podría llevar a que se le incluya en una lista de vigilancia o a que se le considere como objetivo inmediato para una sentencia de cárcel.

Estafas algunos supuestos servicios, como el caso de "sicarios" profesionales, pueden ser estafas diseñadas para sacar provecho de clientes dispuestos. Varios informes han sugerido que la Web oscura ofrece muchos servicios ilegales, desde asesinatos pagados hasta tráfico sexual y de armas.

Algunas de estas son amenazas conocidas y establecidas que circulan en este rincón de la Web. Sin embargo, otros pueden estar aprovechando la reputación de la Web oscura para engañar a los usuarios con grandes sumas de dinero. Además, algunos usuarios de la Web oscura pueden intentar llevar a cabo estafas de Phishing para robar su identidad o información personal con fines de extorsión.

Protección del Usuario Final Frente a la Explotación de la Web Oscura Independientemente de que tenga una empresa, sea un padre, una madre o cualquier otro/a usuario/a de la Web, querrá tomar precauciones para mantener su información y su vida privada fuera de la Web oscura.

El control del robo de identidad es fundamental si quiere evitar que su información privada se utilice incorrectamente. Los datos personales, de todo tipo, se pueden distribuir en línea con fines de lucro. Las contraseñas, las di-

recciones físicas, los números de cuentas bancarias y los números de seguridad social circulan en la Web oscura todo el tiempo. Puede que ya sea consciente de que los actores maliciosos pueden utilizarlos para dañar su crédito, participar en robos financieros y secuestrar otras cuentas suyas en línea. Las filtraciones de datos personales también pueden dañar su reputación a través del fraude social.

Las protecciones antimalware y antivirus son igualmente cruciales para evitar que los actores maliciosos se aprovechen de usted. La Web oscura está llena de robos de información de usuarios infectados con Malware. Los atacantes pueden usar herramientas como los Keyloggers para recopilar sus datos, y pueden infiltrarse en su sistema en cualquier parte de la Web. Los programas de seguridad de Endpoints como Kaspersky Security Cloud son soluciones integrales diseñadas para cubrir tanto la supervisión de la identidad como las defensas antivirus.

Cómo Acceder a la Web Oscura de Forma Segura Si tiene una necesidad legítima o viable de acceder a la Web oscura, querrá asegurarse de que está a salvo si decide usarla. Algunos consejos para acceder con seguridad a la Web oscura:

- Usar una máquina virtual[96], ya que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados por ellas. Estos procesos no pueden escaparse de esta "computadora virtual". De esta forma podemos ejecutar uno o más sistemas operativos -Linux, Mac, Windows- desde nuestro sistema operativo habitual sin necesidad de instalarlo directamente en nuestra computadora y sin la preocupación de que se desconfigure el sistema operativo huésped o a las vulnerabilidades del sistema virtualizado, ya que podemos aislarlo para evitar que se dañe y puede ser desechado al terminar las búsquedas.

[96] Una máquina virtual dispone de todos los elementos de un equipo de cómputo real, de disco duro, memoria RAM, unidad de CD o DVD, tarjeta de red, tarjeta de vídeo, etc., pero a diferencia de un equipo de cómputo real estos elementos en vez de ser físicos son virtuales. Así, una vez instalado un sistema operativo en la máquina virtual, podemos usar el sistema operativo virtualizado del mismo modo que lo usaríamos si lo hubiéramos instalado en nuestro equipo de cómputo.

Algunas opciones de manejadores de máquinas virtuales son: Virtualbox, Vmware Workstation Player, Parallels, Windows Virtual PC, QEMU/KVM.

- Elimina o bloquea tu Webcam durante el proceso, para que no puedas ser espiado.
- Actualiza tu sistema operativo y antivirus previamente.
- Activa tu antivirus y Firewall.
- De preferencia usa una VPN
- Confíe en su intuición. Para evitar que le estafen, querrá protegerse con un comportamiento inteligente en la Web. No todo el mundo es lo quien pretende ser en internet. Mantenerse a salvo requiere que vigile con quién habla y qué sitios visita. Siempre debe tomar medidas para alejarse de una situación si algo le resulta extraño.
- Separe su imagen en línea de la vida real. No debe utilizar en ningún otro lugar su nombre de usuario, dirección de correo electrónico, "nombre real", contraseña, e incluso su tarjeta de crédito. Cree nuevas cuentas e identificadores desechables para utilizar si es necesario. Adquiera tarjetas de débito prepago no identificables antes de realizar cualquier compra. No utilice nada que se pueda utilizar para identificarle, bien sea en línea o en la vida real.
- Utilice una supervisión activa de los robos financieros y de identidad. Muchos servicios de seguridad en línea ofrecen ahora protección de la identidad para su seguridad. Asegúrese de aprovechar estas herramientas si las tiene a su disposición.
- Evite explícitamente descargar archivos de la Web oscura. La posibilidad de una infección por Malware es significativamente superior en el territorio sin ley que ofrece la Web oscura. El análisis de archivos en tiempo real de un programa antivirus puede ayudarle a comprobar los archivos entrantes en caso de que decida descargarlos.
- Desactive ActiveX y Java en cualquier configuración de red disponible. Es bien sabido que los ciberdelincuentes investigan y explotan estas plataformas. Debido a que está navegando por una red llena de amenazas maliciosas, querrá evitar este riesgo.
- Utilice una cuenta de usuario local secundaria, sin derechos administrativos, para todas sus actividades diarias. La cuenta nativa en la

mayoría de los ordenadores tendrá permisos administrativos completos de forma predeterminada. La mayoría del Malware se aprovecha de estos derechos para ejecutar sus funciones. Por ello, puede frenar o detener el progreso de la explotación al limitar la cuenta que está utilizando a privilegios estrictos.

- Restrinja siempre el acceso a su dispositivo habilitado para Tor. Proteja a los usuarios de su equipo para que no corran el riesgo de encontrarse con algo que nunca nadie debería ver. Visite la Web profunda si le interesa hacerlo, pero no permita nunca que los niños se acerquen a ella.

9.5 Cómo Podemos Entrar en la Internet Oculta

Para ingresar debemos usar algún servicio de red tipo Tor (The Onion Router). Esta red funciona de una forma especial, en este caso se basa en una técnica de capas que sirve para proteger las comunicaciones y tratar de garantizar el anonimato en Internet. La red Tor trabaja cifrando la información a su entrada y la descifra a la salida de dicha red, esto es conocido como Onion Routing. Además, el navegador Tor es el encargado de resolver los dominios *.onion* y mostrar al internauta las Webs de la internet oculta (la velocidad de conexión a cualquier nodo de la red es baja por la cantidad de conexiones utilizadas para garantizar el anonimato).

Tor respecto al navegador es mejor utilizar el navegador Tor Browser que utiliza la red Tor. Lo primero que tenemos que hacer es descargarlo desde su sitio Web oficial. Es un navegador multiplataforma y lo tenemos para Windows, Linux, MacOS y Android. Una vez terminada la instalación lo ejecutamos. Aquí lo único que tenemos que hacer es pulsar Conectar para enrutar tu tráfico a través de la red Tor. Si queremos, también podemos activar la casilla «Siempre conectar automáticamente» y se iniciará el navegador Tor conectado a la red que lleva su nombre.

Invisible Internet Project está disponible también para Windows, macOS, Linux y Android, exactamente igual que Tor Browser. Además de poder acceder a la Deep Web, también lo podemos utilizar como un navegador Web normal. En este caso, no se basa en la red Tor -que también se puede utilizar-, sino que se utiliza una red propia para conseguir que

naveguemos de forma anónima. Todas las conexiones son cifradas, incluyendo las claves públicas y privadas, y el tráfico se 'enruta', como en Tor Browser, para impedir el seguimiento. Por otro lado, ofrece como particularidad el almacenamiento de archivos de forma descentralizada.

Whonix esta opción tiene una disponibilidad ligeramente más limitada, porque solo lo podemos descargar e instalar en Windows, macOS y Linux, nada de dispositivos móviles. Está basado en el mismo código fuente de Tor Browser, así que si estamos acostumbrados a él nos parecerá sencillo el cambio. A nivel más interno, sin embargo, hay cambios importantes como un sistema para evitar que en cualquier tipo de actividad se descubra la dirección IP del usuario. Para ello se usa una máquina virtual, con una LAN virtual interna, que se comunica en exclusiva con el router. Ni siquiera un sofisticado Malware, según sus desarrolladores, sería capaz de descubrir la dirección IP del ordenador incluso teniendo privilegios como administrador sobre el sistema. Pero no es un navegador Web convencional, sino parte del sistema operativo Whonix, que se ejecuta dentro de una máquina virtual y tiene más herramientas útiles como, por ejemplo, utilidades de ofimática.

Subgraph OS esta última opción, de nuevo, no es un navegador Web convencional, sino que se trata de un sistema operativo completo. Así que, de nuevo, lo podemos utilizar en cualquier ordenador. Del mismo modo que Whonix, el código fuente sobre el que parte el sistema operativo es el de Tor Browser, pero también cuenta con un sofisticado sistema de múltiples capas para la protección de la seguridad del usuario y su identidad. Cifrado de meta-proxy, por ejemplo, o el cifrado del sistema de archivos entre muchos otros, y con aislamiento en Sandbox para aplicaciones.

Como ya mencionamos, para entrar a la Deep Web debemos hacerlo a través de los buscadores DuckDuckGo, Torch, The Hidden Wiki y más que veremos a continuación.

The Hidden Wiki desde un punto estricto no lo podríamos considerar como un buscador. No obstante, como contiene un listado actualizado de enlaces de los principales sitios de la Deep Web, hace que la tengamos que prestar mucha atención como punto de partida. El motivo porque tiene gran importancia en la red Tor, es porque las URL que se utilizan con .onion

cambian muy a menudo. Sin embargo, en el apartado Introduction Points podremos acceder Deep Web con los buscadores si pulsamos sobre sus enlaces. En resumen, de The Hidden Wiki nos proporciona una excelente herramienta por si se cambian las URL de las diferentes Webs, es una forma de tener todo centralizado.

DuckDuckGo podemos definirlo como un buscador independiente, cuya principal seña de identidad es que no recopila información sobre sus usuarios. Su filosofía se centra en la privacidad de los internautas. Este buscador también existe en la Web habitual que todos conocemos, de hecho, si quieres proteger tu privacidad y seguridad a la hora de navegar por la Web «normal», es recomendable usar DuckDuckGo. Un elemento que le diferencia de otros motores de búsqueda es que no funciona a partir de las búsquedas anteriores, las preferencias o la ubicación del usuario. En la gran mayoría de resultados obtendremos los mismos que con un buscador convencional, pero protegido con la privacidad que ofrece la red Tor.

Torch podemos considerarlo como uno de los mejores buscadores de la Deep Web y también como uno de los más longevos y populares. Este buscador asegura que tiene más de un millón de páginas indexadas en su base de datos. Si queremos obtener cosas poco habituales, puede ser una opción aunque a veces te encuentras con Links caídos porque no han sido actualizados correctamente, no obstante, hay una grandísima cantidad de información para poder navegar por la Deep Web.

Ahmia es otro buscador muy útil para encontrar mucha información en la Deep Web, con los anteriores buscadores y con Ahmia tenemos todos los ingredientes para empezar a usar la red Tor y navegar por la Deep Web. Una cosa por la que destaca Ahmia es por tener un diseño más cuidado que la mayoría de los sitios que encontramos en la Deep Web. Una de sus características, es que tiene un sistema de lista negra, donde todo aquello que encuentre que sea excesivamente censurable, lo elimina para no herir la sensibilidad del usuario. Nos encontramos con una página Web bastante rápida y que no hará que estemos esperando durante mucho tiempo.

NotEvil otro buscador que podemos utilizar es NotEvil. Su funcionamiento es muy sencillo, bastará que delimiten bien con las palabras clave aquello

que estás buscando. Únicamente tendrás que utilizar la barra del buscador y pulsar el botón Search para realizar tus consultas. En este caso tiene todo tipo de enlaces que te llevarán a páginas que te resulten útiles, y además, no contiene anuncios que molesten. Por otra parte, su interfaz es simple y te resultará bastante sencillo adaptarte a ella.

Otras alternativas a la red Tor para ingresar a la Deep Web son:

ZeroNet una de las Darknets alternativas a Tor es ZeroNet, una red abierta, gratuita y sin censura que utiliza la criptografía Bitcoin y la red BitTorrent. Debemos tener claro que el contenido es distribuido directamente a otros visitantes sin ningún servidor central y que todo funciona con dominios *.bit*. Para empezar con ella, debemos descargar el ejecutable de ZeroNet para Windows, macOS o Linux.

Freenet es un Software gratuito que le permite compartir, navegar y publicar archivos de forma anónima páginas, además de chatear y olvidarnos de la censura. Se trata de una red P2P o descentralizada que nació en el año 2000. Todos sus nodos están cifrados y hacen tremendamente difícil identificar a la persona que demanda un contenido. Los usuarios contribuyen a la red dando ancho de banda y una parte de su disco duro. Empezaremos descargando el instalador de Freenet desde su web oficial. Este lo tenemos disponible para Windows, macOS y Linux. El proceso de instalación es muy sencillo y, una vez finalizado, se abrirá Freenet con nuestro navegador habitual.

I2P es una red anónima construida sobre Internet. Permite a los usuarios crear y acceder a contenido y crear comunidades en línea en una red distribuida y dinámica. Su objetivo es proteger la comunicación y resistir el monitoreo por parte de terceros, como los ISP. Acceder también requiere de la instalación de un Software especial. I2P está disponible para Windows, macOS, Linux y Android.

Tal y como hemos visto en esta sección, disponemos de muchos métodos para ingresar a la Deep Web y múltiples buscadores para navegar por ella cómodamente, eso sí, habrá algunos enlaces que no funcionen o que la carga de las diferentes Webs sea realmente lenta, por lo que tendrás que tener

paciencia. Es el precio a pagar por el anonimato, la privacidad y la seguridad de las comunicaciones.

9.6 ¿Cómo funciona TOR?

El nombre TOR son las siglas de The Onion Router (el enrutado Cebolla), y es posiblemente la principal y más conocida Darknet de Internet. El objetivo de este proyecto es el de crear una red de comunicaciones distribuida y superpuesta al Internet convencional. Las Dark Webs que puedes encontrar en la Darknet de TOR se diferencian por tener el dominio *.onion*.

Tor es una red que implementa una técnica llamada Onion Routing (enrutado cebolla en castellano), diseñada con vistas a proteger las comunicaciones en la Marina de los Estados Unidos. La idea es cambiar el modo de enrutado tradicional de Internet para garantizar el anonimato y la privacidad de los datos.

El enrutado tradicional que usamos para conectarnos a servidores en Internet es directo. Por ejemplo, si quieres leer una Web tu ordenador se conecta de forma directa a sus servidores. La ruta es relativamente sencilla: de tu máquina a tu Router, de ahí a los enrutadores de tu ISP (proveedor de Internet) y después directos a los servidores de la Web que estás visitando.

Onion Routing, que consiste en enviar los datos por un camino no directo utilizando diferentes nodos. Primero, la máquina A, que quiere enviar el mensaje a B, calcula una ruta más o menos aleatoria al destino pasando por varios nodos intermedios. Después, consigue las claves públicas de todos ellos usando un directorio de nodos.

Usando cifrado asimétrico, la máquina A cifra el mensaje como una cebolla: por capas. Primero cifrará el mensaje con la clave pública del último nodo de la ruta, para que sólo él lo pueda descifrar. Además del mensaje, incluye (también cifradas) instrucciones para llegar al destino, B. Todo este paquete, junto con las instrucciones para llegar al último nodo de la lista, se cifra de nuevo para que sólo lo pueda descifrar el penúltimo nodo de la ruta.

Pero tampoco es un método infalible, ya que analizando los tiempos a los que se reciben y envían los paquetes en cada nodo se podría llegar a saber, con mucho tiempo y dedicación, qué máquinas se están comunicando.

Además, de cara al usuario convencional está la molestia de que el precio a pagar por la privacidad y seguridad es la velocidad,

Tor cifra y anonimiza tu conexión al pasarlo a través de 3 repetidores (Relays). Los repetidores son servidores operados por diferentes personas y

organizaciones de todo el mundo.

Diferencias Entre Repetidores (Relays) o Nodos de Tor Los repetidores Tor también se conocen como "enrutadores" o "nodos". Reciben tráfico en la red Tor y lo transmiten.

Hay 3 tipos de relés que puede ejecutar para ayudar a la red Tor:

- Repetidores intermedios (Guard and Middle Relay)
- Repetidores de salida (Exit Relay)
- Puentes (Bridges)

Para mayor seguridad, todo el tráfico de Tor pasa por al menos tres repetidores antes de llegar a su destino. Los dos primeros repetidores son repetidores intermedios que reciben tráfico y lo pasan a otro repetidor. Los repetidores intermedios aumentan la velocidad y la robustez de la red Tor sin hacer que el propietario del repetidor parezca la fuente del tráfico. Los repetidores intermedios anuncian su presencia al resto de la red Tor, para que cualquier usuario de Tor pueda conectarse a ellos.

1- Guardián y Nodo Intermedio (también conocido como repetidores sin salida) un repetidor de protección es el primer repetidor de la cadena de 3 repetidores que forman un circuito Tor. Un relevo intermedio no es ni un guardia ni una salida, sino que actúa como el segundo salto entre los dos.

2- Repetidor de Salida (Exit Relay) el repetidor de salida es el repetidor final en un circuito Tor, el que envía tráfico a su destino. Los servicios a los que se conectan los clientes de Tor (sitio Web, servicio de chat, proveedor de correo electrónico, etc.) verán la dirección IP del repetidor de salida en lugar de la dirección IP real del usuario de Tor.

3- Puente (Bridge) el diseño de la red Tor significa que la dirección IP de los repetidores Tor es pública. Sin embargo, una de las formas en que los gobiernos o los ISP pueden bloquear Tor es mediante la lista de bloqueo de las direcciones IP de estos nodos públicos de Tor. Los puentes Tor son nodos

de la red que no figuran en el directorio público de Tor, lo que dificulta que los ISP y los gobiernos los bloqueen.

Los puentes son útiles para los usuarios de Tor bajo regímenes opresivos o para las personas que quieren una capa adicional de seguridad porque les preocupa que alguien reconozca que están contactando una dirección IP pública de retransmisión de Tor. Varios países, incluidos China e Irán, han encontrado formas de detectar y bloquear las conexiones a los puentes Tor. Los transportes conectables, un tipo especial de puente, abordan esto agregando una capa adicional de ofuscación.

Navegar con Tor (Tor Browser) es extremadamente sencillo gracias a que tiene un navegador preparado para conectarte sin grandes problemas. Lo primero que tienes que hacer es ir a la página de Tor Browser, y pulsar sobre el icono de tu sistema operativo para descargártelo. Se trata de un navegador basado en Firefox especialmente creado para entrar en TOR sin tener que configurar nada. Sólo lo abres y te conecta automáticamente.

Elige la carpeta de destino e instálalo, después ejecuta el navegador. Verás que este no se abre automáticamente, sino que primero te muestra una ventana que te indica que puedes conectarte o configurar la conexión. Pulsa en el botón Connect, y cuando termine el proceso de conexión Tor Browser se abrirá y podrás navegar con él tanto por la Clearnet como por la red de Tor. Viene con el buscador DuckDuckGo configurado para encontrar también páginas *.onion*, el dominio de las Webs de esta Darknet.

Ayudar a los Usuarios Censurados ejecuta un puente Tor, los puentes son repetidores Tor privados que sirven como trampolines hacia la red. Cuando la red Tor está bloqueada, los usuarios pueden obtener un puente para eludir la censura. Gracias a la comunidad de operadores de puentes, los usuarios de China, Bielorrusia, Irán y Kazajstán pueden conectarse a la red Tor y acceder a Internet libre y abierto.

Actualmente hay aproximadamente 1200 puentes, 900 de los cuales admiten el protocolo de ofuscación obfs4. Desafortunadamente, estas cifras han ido disminuyendo desde principios del año 2021. No es suficiente tener muchos puentes: eventualmente, todos ellos podrían encontrarse en listas de bloqueo.

Configuración de un Puente para configurar un puente *obfs4*, consulte las instrucciones de instalación. Hay guías para varias distribuciones de Linux, FreeBSD, OpenBSD y Docker. Ten en cuenta que un puente *obfs4* necesita tanto un TOR abierto como un puerto *obfs4* abierto. Para unirse a la campaña de puentes, debe seguir estos requisitos:

- Dirección IPv4 estática. Aunque los puentes Tor pueden operar detrás de direcciones IP dinámicas, este escenario no es tan óptimo si se piensa en otros que necesitan configurar regularmente las nuevas direcciones IP manualmente. IPv6 es definitivamente una ventaja, pero no es obligatorio.

- Transporte enchufable Obfs4 configurado. Como se trata del transporte enchufable con mayores probabilidades de pasar por la censura global, se opta por este.

- Tiempo de actividad 24 horas al día, 7 días a la semana. Servir a la red las 24 horas del día, los 7 días de la semana es vital para los puentes, ya que aquellos que realmente necesitan solucionar la censura dependen de que Tor esté siempre disponible.

Otras Formas de Ayudar Si no es lo suficientemente técnico para ejecutar un puente, pero desea ayudar a los usuarios censurados, hay otras formas en las que puedes ayudar:

- Ejecutar un Proxy Snowflake. No necesita un servidor dedicado y se puede ejecutar un Proxy simplemente instalando una extensión en tu navegador. La extensión está disponible para Firefox y también para Chrome. No hay necesidad de preocuparse por los sitios Web a los que acceden las personas a través de tu proxy. Tu dirección IP de navegación visible coincidirá con su nodo de salida de Tor, no con el tuyo.

Todo el Sistema Operativo vía Tor con Tails

- Tails es el sistema operativo portátil que te protege de la vigilancia y la censura.

- Evita la vigilancia, la censura, la publicidad, y los virus

- Tu computadora segura en cualquier lugar

Tails usa la red Tor para proteger tu privacidad en línea y ayudarte a evitar la censura. Disfruta de Internet como debería ser.

Apaga tu ordenador e inicia en tu memoria USB con Tails en lugar de iniciarla con Windows, macOS o Linux. Tails no deja rastros en la computadora cuando la apagas.

Tails incluye una selección de aplicaciones para trabajar en documentos confidenciales y para comunicarse de forma segura.

¿Quién usa Tails?

- Activistas usan Tails para ocultar sus identidades, evitar la censura y comunicarse de manera segura.
- Periodistas y sus fuentes usan Tails para publicar información confidencial y acceder a internet desde lugares inseguros.
- Sobrevivientes de violencia doméstica usan Tails para escapar de la vigilancia en casa.
- Tú: cuando necesites privacidad adicional en este mundo digital.

Tor para Todo con TAILS todo lo que haces en internet desde Tails pasa por la red Tor. Tor cifra y anonimiza tu conexión, los repetidores son servidores operados por diferentes personas y organizaciones de todo el mundo.

10 Internet y Puertos

Internet (el internet o, también, la internet) es un conjunto descentralizado de redes de comunicaciones interconectadas, que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyen una red lógica única de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California (Estados Unidos).

Uno de los servicios que más éxito ha tenido en internet ha sido la World Wide Web (WWW o la Web), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Esta fue un desarrollo posterior (1990) y utiliza internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia –telefonía (VoIP), televisión (IPTV)–, los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

¿Qué es un puerto? es un pequeño código que se utiliza como punto de acoplamiento en nuestra máquina desde el cual podemos comunicarnos remotamente con otra máquina.

¿Qué es un puerto de Hardware? es un punto de conexión en modo periférico físico a una máquina desde otro dispositivo.

¿Qué es un Socket? se denomina Socket a la combinación de puerto de Software y dirección IP.

¿Cuántos puertos existen el Linux? el rango de puertos va de 0 a 65,535, por tanto tenemos 65,536 puertos.

¿Por qué solo tenemos 65,536 puertos? esto se debe a la limitación TCP/IP, donde cada número de puerto tiene un tamaño de solo 16 bits. Esto equivale a 2^{16}.

¿Qué puertos son los predeterminados? los puertos predeterminados y más utilizados, van del 0 a 1,023 (2^{10} puertos). Otras herramientas usan el resto de los puertos.

¿Qué es un puerto predeterminado? es un puerto designado para un servicio particular, como servidor web (80), servidor de correo (25), servidor SSH (22), etc.

¿Es posible modificar un puerto predeterminado? la respuesta es clara, si se puede. Tan solo debemos modificar el puerto de escucha en el archivo de configuración del servicio que nos interese.

¿Cuántos números de protocolos existen en TCP/UDP? hay que tener cuidado en no confundir los protocolos con los números de puerto, en TCP hay 6 y en UDP hay 17.

¿Dónde podemos ver información sobre los puertos? para ello, podemos hacer:

```
$ cat /etc/services
```

Diferencias entre TCP y UDP Cuando hablamos de protocolos de internet en tráfico, los usuarios pueden elegir entre una configuración TCP o UDP. Las características y funciones de TCP vs UDP son diferentes, cada protocolo tiene sus ventajas, desventajas y posibles problemas.

Dicho esto, UDP es mucho más rápido, aún así muchos sistemas siguen dependiendo de TCP para descargar paquetes de datos. En este artículo echaremos un vistazo a los dos protocolos, pero recordemos que antes de decidirnos por uno u otro, deberemos conocer en profundidad nuestras necesidades.

El protocolo de control de transmisión (TCP) está orientado a la conexión, esto quiere decir que una vez que se establece la conexión, los datos se transmiten en dos direcciones. Este protocolo tiene la capacidad de verificar posibles errores, esta fórmula nos garantiza que los datos se entreguen en el orden enviado.

Dicho lo anterior, TCP es el protocolo perfecto para transferir información relacionada con páginas Web, imágenes fijas y archivos de datos. El uso de la retroalimentación propia del protocolo genera una sobrecarga en la red, que se traduce en un mayor consumo de ancho de banda.

El protocolo de datagramas de usuario (UDP) es un protocolo de internet mucho más simple. No requiere de servicios de recuperación y verificación de errores. Tampoco existe consumo extra al abrir una conexión, mantenerla abierta o terminarla; Los datos se envían de forma continua al destinatario, independientemente de si los recibe o no.

Además, UDP admite el flujo de paquetes constante, es la gran diferencia sobre TCP. La conexión TCP, está obligada a reconocer un conjunto de paquetes (sea confiable o no), por lo tanto, se genera una retransmisión en cada reconocimiento cuyo resultado sea la pérdida de paquetes. El protocolo UDP evita estos consumos, por tanto, el efecto-resultado nos aporta una velocidad mucho más eficiente si hablamos de ancho de banda.

Las aplicaciones Web y de escritorio (de comunicación) priorizan UDP sobre TCP para el transporte de medios en tiempo real.

10.1 Escaneo de Puertos

La herramienta nmap (Abreviatura de Network Mapper) Es la mejor en línea de comandos en Linux (también disponible para *Windows* y *Mac OS X*) para realizar funciones de auditoría y seguridad de redes, rastreo y análisis en busca de sistemas para elaborar un inventario de red, etc. Todo esto de forma gratuita y bajo licencia Open Source. Lanzando un escaneo de puertos de red (1-65,535) TCP y UDP que corresponden a uno o más servicios que se corren en un sistema o servidor. Con nmap podemos visualizar una gran cantidad de información: Hosts activos en la red, sistema operativo que están ejecutando, puertos y servicios abiertos a través de la red, tipos de *Firewall* que están utilizando. Para los recelosos de la línea de comandos, existe la opción de utilizar nmap con GUI, para ello está *Zenmap*.

Este comando puede ser una valiosa herramienta de diagnóstico para los administradores de redes, mientras que también puede ser una herramienta de reconocimiento potente para la comunidad[97] *Black-hat (Hackers, Crackers,*

[97] El escaneo lo puede hacer cualquier usuario sin privilegios de administrador, pero hay algunas opciones reservadas para el usuario *root*.

Script Kiddies, etc.).

¿Por qué escanear puertos contribuye a la seguridad de tu sistema? los puertos desempeñan una función destacada a la hora de que los paquetes de datos encuentren el camino para alcanzar los objetivos deseados. En este sentido, funcionan como interfaz entre equipos de cómputo y servicios o programas del sistema y son usados por los protocolos de red como TCP y UDP. En combinación con la dirección IP, los puertos permiten al sistema operativo no solo saber a qué equipo de cómputo ha de enviar el flujo de datos sino también a qué aplicación ha de entregar los paquetes.

Curiosidades sobre los puertos A cada puerto se le asigna un número comprendido entre el 0 y el 65,535[98]. A este respecto, pueden diferenciarse tres áreas:

- Los puertos que van desde el número 0 al 1023 reciben la denominación de puertos estandarizados y la internet Assigned Numbers Authority (IANA) asigna protocolos fijos y otros recursos a la mayoría de ellos. De esta manera, por ejemplo, se ha reservado el puerto 80 para las conexiones HTTP y, por lo tanto, este se convierte en el puerto decisivo para las solicitudes realizadas a través del servidor Web.
- Los números de puerto que van desde el 1,024 hasta el 49,151 están destinados normalmente a servicios registrados, aunque se asignan también a clientes, en especial por parte de GNU/Linux.
- Los puertos comprendidos entre los números 49,152 y 65,535 son los que otorgan los sistemas operativos a los programas cliente de manera dinámica.

[98] En Debian GNU/Linux se puede conocer los puertos TCP y UDP de los principales servicios, mediante:

```
$ cat /etc/services
```

y la dirección IP de la máquina que uso:

```
$ ip address
```

Para establecer una conexión a través de un puerto determinado este debe estar abierto, es decir, libre. Especialmente en lo referente a la transferencia de datos en internet, esto indica, como es lógico, que hay un gran número de puertos abiertos, lo que lleva aparejado ciertos problemas: cada puerto abierto se convierte en un posible acceso para atacantes, en caso de que la aplicación correspondiente presente brechas de seguridad. Por este motivo, es necesario tener siempre en mente cuáles son los puertos que están abiertos en tu sistema y cuáles son las aplicaciones que hay detrás del tráfico de datos. Los escáneres de puertos son los mejores recursos con los que puedes detectar la presencia de puertos activos.

¿Qué es el escaneo de puertos? por escaneo de puertos se entiende aquel procedimiento que tiene como objetivo analizar los puertos abiertos de un sistema informático con la ayuda de herramientas especiales. Para poder llevar a cabo dicho escaneo, no es necesario registrarse en el sistema de destino, sino solo estar conectado a él, por ejemplo, a través de una red local o de internet. Con ayuda de los analizadores de puertos (*Port Scanners)* se envían, a modo de prueba, paquetes de datos especiales a los diferentes puertos y se obtienen las correspondientes respuestas o mensajes de error que la herramienta analiza y evalúa. Independientemente de la funcionalidad del programa de Port Scanning que se use, no solo se pueden obtener datos acerca de cuáles son los puertos abiertos o cerrados, sino también sobre el sistema operativo que usa el equipo de destino, sobre el tiempo que hace que el PC permanece encendido o sobre los servicios o aplicaciones que utilizan los puertos correspondientes.

El escaneo de puertos representa un medio muy eficiente al que los administradores de sistemas pueden recurrir para controlar el tráfico de datos de una red y para filtrar sus posibles debilidades. En algunos casos determinados, también se pueden solucionar problemas de red concretos. Debido a que las herramientas no tienen una influencia significativa en la capacidad de rendimiento de los sistemas que se examinan, pueden utilizarse sin vacilaciones para dichas medidas de seguridad. También en el ámbito doméstico puede ser de utilidad el método del escáner de puertos, y es que en cuanto se instalan y se usan aplicaciones que requieren una conexión a internet, también se abren puertos automáticamente, siempre que el Firewall no lo impida.

El escaneo de puertos ayuda a mantener una visión general y muestra los

puertos que ya han dejado de ser necesarios y que, en consecuencia, pueden cerrarse para minimizar los riesgos que pueden afectar a la seguridad. Pero hay que recordar siempre, que todos los resultados obtenidos por las herramientas automáticas deben ser revisados por un profesional en Hacking Ético y Pruebas de Penetración. Pues casi siempre existen falsos positivos.

¿Cómo funciona el escaneo de puertos exactamente? para escanear puertos existen normalmente diferentes métodos, la mayoría de los cuales gira en torno al protocolo de conexión TCP. Para comprender cuáles son los procesos básicos que tienen lugar mediante el escaneo de puertos, es de utilidad echar un vistazo a los aspectos generales del establecimiento de la conexión mediante el protocolo TCP:

- En el marco del proceso denominado negociación en tres pasos (3-Way Handshake), el cliente envía, en primer lugar, un paquete SYN (Synchronize = "sincronizar") al puerto de destino correspondiente.
- Si este consigue llegar hasta una aplicación, recibe un paquete SYN/ACK combinado (Synchronize Acknowledge = "confirmar sincronización") que confirma el establecimiento de la conexión.
- El cliente responde en el tercer y último paso con un paqueteACK (Acknowledge = "confirmar"), por lo que se establece la conexión y ya puede comenzar el intercambio de datos.

Si se establece el contacto con un puerto cerrado, el cliente recibe en el segundo paso un paquete con el flag RST (reset = "restablecer") como respuesta, por lo que se interrumpe la negociación.

Puesto que el intercambio de datos con las diversas aplicaciones resultaría por un lado muy costoso y por otro muy complejo, el escáner de puertos solo está limitado a un sencillo intento de conexión, como ponen de relieve los métodos de escaneo que te presentamos a continuación.

TCP SYN en este caso se puede hablar de un escaneo medio abierto, ya que este no tiene como objetivo el establecimiento de una conexión *TCP* completa. En esta modalidad se pueden enviar paquetes *SYN* habituales a cada uno de los puertos con el port scanner, tras lo que se espera una respuesta por parte del Host de destino. Si este responde con un paquete

SYN/ACK, esto indica que el puerto correspondiente está abierto y que es posible establecer la conexión. Si la respuesta consiste en un paquete *RST*, esto indicará que el puerto está cerrado. Si el Host de destino no ha enviado todavía una respuesta, todo indica que se ha interpuesto un filtro de paquetes, como, por ejemplo, un Firewall. Los escaneos *TCP SYN* no son visibles para las aplicaciones revisadas y no generan, por lo tanto, datos de registro, de ahí que también reciben el nombre de stealth scans ("escaneos sigilosos").

TCP connect si haces uso del escaneo de puertos para llevar a cabo un sondeo del tipo *connect*, en este caso no generas, ni envias los paquetes de datos motu proprio, sino que recurres para ello a la llamada al sistema *connect*. Esta está disponible para casi todos los sistemas operativos y, por ejemplo, el navegador Web también hace uso de ella para establecer la conexión con un servidor. Esta herramienta de escaneo no está implicada en el establecimiento de la conexión, sino que es el sistema operativo el encargado de ello, el cual puede o bien crear una conexión con éxito y confirmar, por lo tanto, que el puerto está abierto o fracasar en el intento e indicar que el puerto correspondiente es un puerto cerrado. Si se establece la conexión por completo, en los archivos de registro de las aplicaciones con puertos abiertos se ve fácilmente si se utilizó este método de sondeo, pero no qué programas de filtrado se utilizan. Sin embargo, si careces de los derechos para enviar paquetes de datos en bruto, el método del *TCP* connect es una alternativa útil al escaneo *SYN*.

TCP FIN, Xmas y Null con estos tres métodos de escaneo de puertos también se puede diferenciar entre los puertos abiertos y los cerrados. Para ello se pueden aplicar los dos principios básicos registrados en las *RFC* (Request For Comments) del TCP. Por un lado, un puerto cerrado siempre tiene que responder a los paquetes entrantes que no sean paquetes *RST* con un paquete *RST* propio. Por otro, el puerto abierto tiene que ignorar todos los paquetes no marcados como *SYN, RST* o *ACK*. Los tres métodos de escaneo anteriormente mencionados se hacen eco de esta situación a la hora de sondear sistemas de conformidad con las publicaciones *Request For Comment* con sus paquetes individuales:

- El escaneo *Null* no coloca ninguna marca especial.
- En el *FIN*, el port scanner envía paquetes *FIN* (finish= terminar).

- Los escaneos *Xmas* combinan las marcas *FIN*, *PSH* (push= empujar) y *URG* (urgent= urgente), por lo que "iluminan" el paquete del mismo modo en que lo hace un árbol de Navidad.

Estos tres métodos se comportan exactamente de la misma manera. Los paquetes de prueba que se envían se ocupan de que, a causa de las disposiciones de *RFC*, un puerto cerrado responda con un paquete *RST* y de que un puerto abierto no muestre ninguna reacción por su parte. No obstante, debido a que sólo algunos Routers transmiten mensajes de error cuando se filtra un puerto, también puede darse una ausencia de reacción en el caso de un puerto filtrado. Aunque estos procedimientos resultan más discretos que los escaneos *SYN*, estos tienen la desventaja de que no funcionan cuando los sistemas no se ciñen exactamente al protocolo *RFC*. Windows se constituiría en este caso como el representante más importante.

UDP en los escaneos *UDP* se envían encabezados *UDP* vacíos y sin datos a todos los puertos de destino. Si un servicio responde con un paquete *UDP*, queda confirmado que el puerto que le pertenece está abierto. Si el Router envía al port scanner el mensaje de error "Port unreachable" (Type 3, Code 3), este sabrá que el puerto está cerrado. Otros tipos de mensajes de error informan de que un filtro de paquetes bloquea el puerto. El gran problema que se deriva de escanear puertos con *UDP* es que requiere mucho tiempo, ya que en numerosos sistemas, la tarea de emitir los correspondientes mensajes de error puede tardar mucho tiempo por motivos de seguridad y los puertos abiertos solo responden de forma muy irregular. El núcleo de Linux limita el número de mensajes a, por ejemplo, uno por segundo, lo que significa que se pueden escanear 65.535 puertos en unas 18 horas.

Por qué el escaneo de puertos no es siempre legal nmap no solo es popular entre los usuarios de equipos de cómputo, sino también en el gremio ciberdelincuentes. El control de los puertos no siempre se realiza de manera legal. Si se concluye en última instancia con un intento de ataque, como puede ser lo que se conoce en el lenguaje técnico como aprovechamiento de una brecha de seguridad, se puede incurrir en actos punibles. Algo menos clara parece la situación legal cuando, por ejemplo, se paraliza un sistema informático debido a un escaneo de puertos intensivo. Ya que los métodos de control pueden suponer una gran carga para el sistema de destino debido

a la alta frecuencia de peticiones de conexión, esto puede ocasionar, entre otras consecuencias, el bloqueo del sistema.

Además, también es posible que los responsables del sistema de destino se den cuenta de los planes antes del fallo general y lo consideren como un primer paso para llevar a cabo el ataque. En este sentido, no pueden perderse de vista las consecuencias legales. En caso de provocar una sobrecarga en el sistema externo de manera intencionada se hablaría de los famosos ataques *DoS* y *DDoS*, que casi con total seguridad pueden incurrir en un procesamiento penal.

De la información anteriormente expuesta se deduce que es conveniente asegurarse de que se tiene la autorización para realizar el denominado escaneo de puertos en el sistema correspondiente. También es aconsejable usar esta técnica únicamente por motivos de seguridad y no por pura curiosidad. Las medidas mostradas para poner en marcha el escaneo de puertos ponen de relieve la importancia de no perder de vista los puertos tanto del propio sistema o del equipo de cómputo de red como de los servicios a los que se puede acceder a través de ellos.

Instalación de nmap para su instalación, usamos:

```
# apt install nmap
```

también en caso de ser necesario podemos instalar una interfase gráfica para *nmap* usando:

```
# apt install nmapsi4
```

Ejemplos de Escaneo de Puertos la herramienta nmap ofrece varios métodos para analizar un sistema. En este ejemplo, realizo una exploración utilizando el nombre de Host para averiguar todos los puertos abiertos[99], servicios y la dirección MAC del sistema.

Si es nuestra propia máquina, primero debemos conocer el *IP* de ella, para ello usamos en comando *ip*, mediante:

```
$ ip address
```

[99] En ciertas redes no esta permitido hacer revisión de puertos, pues se considera un ataque a los equipos que la integran, llegando a deshabilitar de la red al equipo que lo realizo.

con esta dirección *IP* (supongamos 192.168.0.2), podemos ver los puertos de la máquina que tiene abiertos hacia el exterior, usando:

```
$ nmap 192.168.0.2
```

y podemos ver además los puertos que tenemos abiertos para uso interno, mediante:

```
$ nmap localHost
```

El escaneo lo puede hacer cualquier usuario sin privilegios de administrador, pero hay algunas opciones reservadas para el usuario *root*. Pero por las repercusiones que puede tener el escaneo a equipos de la red, es mejor que se haga por un usuario avanzado.

Otros Programas para Escaneo de Puertos Podemos instalar el programa *iproute2* para realizar el escaneo de puertos, mediante:

```
# apt install iproute2
```

y escaneamos puertos usando:

```
# ss -tulpn
```

Podemos instalar el programa *net-tools* para realizar el escaneo de puertos, mediante:

```
# apt install net-tools
```

y escaneamos puertos usando:

```
# netstat -tilnp
```

Podemos instalar el programa *lsof* para realizar el escaneo de puertos, mediante:

```
# apt install lsof
```

y escaneamos puertos usando:

```
# lsof -nP -iTCP -sTCP:LISTEN
```

Otras opciones son: Angry IP Scanner, Sandmap, Unicornscan, Netcat, Zeus, Vault, entre otros.

10.2 Cortafuegos

Cortafuegos o *Firewall* en inglés, es una solución diseñada para proteger tu equipo de cómputo. Son tipos de protección que posiblemente ya estés utilizando sin darte cuenta, pero eso no quiere decir que debas despreocuparte y no conocer lo que hacen y lo que no hacen. Todos los sistemas operativos tienen cortafuegos, tanto en cuanto son simples normas encargadas de reconducir el tráfico exterior de información hacia nuestro sistema operativo.

Empezaremos explicando de forma sencilla y entendible qué es un cortafuegos y para qué sirve exactamente. Luego, pasaremos a explicar cómo funcionan diciéndote los dos tipos principales de cortafuegos, y terminaremos recordándote que no debes delegar 100% en ellos ni ninguna otra solución para proteger tu equipo de cómputo.

Qué es un Cortafuegos y Para qué Sirve El cortafuegos en el mundo de la informática es un sistema de seguridad para bloquear accesos no autorizados a un equipo de cómputo mientras sigue permitiendo la comunicación de tu equipo de cómputo con otros servicios autorizados. También se utilizan en redes de equipos de cómputo, especialmente en Intranets o redes locales. Se trata de una de las primeras medidas de seguridad que empezó a implementarse en los equipos de cómputo tras el nacimiento de internet.

Su origen se remonta a finales de la década de los 80, cuando internet daba sus primeros pasos y los primeros Hackers descubrieron que con esta nueva red podían infiltrarse y hacer travesuras en los equipos de cómputo de otras personas, lo que llevó a una serie de importantes violaciones de seguridad y ataques de *Malware*. Internet necesitaba ser más segura para extenderse, por lo que varios investigadores empezaron a desarrollar las primeras versiones de cortafuegos informáticos en 1988 como método para el filtrado de los paquetes digitales que le llegaban a un equipo de cómputo.

Con el tiempo fueron evolucionando para conseguir analizar mejor la información entrante y filtrar las posibles amenazas. La finalidad siempre ha sido la misma que siguen teniendo hoy, la de establecer unos criterios de seguridad, y filtrar todas las comunicaciones que entran o salen del equipo de cómputo para interceptar las que no cumplan con ellos y dejar pasar al resto. Estos criterios van variando y evolucionando con el tiempo para mantenerse actualizados frente a unos ataques también en constante evolución. Es importante que sepas que los cortafuegos no eliminan el Malware que intenta entrar, sólo trata de bloquear su acceso.

Un equipo dedicado de cortafuegos es una máquina segura y confiable que se asienta entre una red privada y una red pública. La máquina cortafuegos se configura con un conjunto de reglas que determinan a qué tráfico de red se le permitirá pasar y cuál será bloqueado o rechazado. En algunas organizaciones grandes, puede que encuentre un cortafuegos localizado dentro de la red corporativa para separar áreas sensibles de la organización de otros empleados. Algunos casos de criminalidad informática acontecen dentro de la misma organización, no sólo provienen de fuera.

Se pueden construir cortafuegos en una variedad de maneras. La configuración más sofisticada involucra un número de máquinas separadas y se conoce como red perimetral. Dos máquinas, denominadas estranguladoras actúan como "filtros" para permitir pasar sólo ciertos tipos de tráfico de red, y entre estos estranguladores residen servidores de red como una pasarela de correo o un servidor intermediario de '*World Wide Web*'. Esta configuración puede resultar muy segura y permite de forma fácil un amplio rango de control sobre quién puede conectarse tanto desde dentro hacia fuera cómo desde fuera hacia dentro. Este tipo de configuración debería ser el utilizado por las grandes organizaciones.

Sin embargo, típicamente los cortafuegos son máquinas únicas que sirven todas estas funciones. Esto es algo menos seguro, porque si hay alguna debilidad en la propia máquina del cortafuegos que le permita a alguien conseguir el acceso al mismo cortafuegos, la seguridad de toda la red habrá sido comprometida. Sin embargo, estos tipos de cortafuegos son más baratos y fáciles de mantener que la configuración más sofisticada descrita arriba.

Cómo Funcionan los Cortafuegos Los cortafuegos pueden ser de dos tipos, pueden ser Software, de Hardware o una combinación de ambos. Esto quiere decir que pueden ser aplicaciones que instales en tu equipo de cómputo o dispositivos que se conecten a él para controlar el tráfico.

Los cortafuegos físicos pueden ser productos independientes o venir directamente integrados en un *Router*. Los independientes se suelen situar entre el punto de acceso a internet y el *Switch* que se encarga de distribuir la conexión entre los equipo de cómputo de una misma red. El hecho de que vaya antes de la distribución de la red entre los equipos significa que todos los que haya en una red interna quedan protegidos. Son buenos para muchos ataques exteriores, sobre todo para las redes internas e Intranets. Esto les convierte en buenas herramientas para empresas y grandes redes. Pero no

son tan seguros con muchos tipos de ataque que vengan a través de otra aplicación, como los troyanos o las amenazas que recibes a través de correos electrónicos fraudulentos.

Los cortafuegos más populares en los usuarios, son los cortafuegos en forma de Software, que son aplicaciones que pueden instalarse en los equipos de cómputo[100]. Su desventaja es que sólo protegen de manera individual a cada equipo de cómputo que los tiene instalados.

Ahora vamos a hablar de sus funciones. Como hemos explicado, los cortafuegos se sitúan entre la red local e internet, y su misión es protegerte bloqueando el tráfico no solicitado o que considere peligroso. Pero puede hacer otras cosas, como aprovechar que analiza el tráfico que entra o sale para configurar filtros para diferentes tipos de tráfico con los que decidir qué hacer con él. En estas configuraciones se pueden hacer muchas cosas, como por ejemplo permitir únicamente las conexiones a servidores de direcciones *IP* concretas, descartando el resto por seguridad. Esto evidentemente a nivel doméstico no es muy efectivo, te impide navegar con facilidad, pero en ámbitos empresariales o más cerrados puede servir.

Al poder analizar el tráfico saliente, también pueden llegar a detectar si hay algún Malware comunicándose con la red, monitorizando el uso de redes empresariales, o filtrando el tráfico. Además, también puede configurarse, por ejemplo, para que sólo el navegador de los equipos de cómputo de una empresa pueda conectarse a internet, bloqueando el acceso del resto de aplicaciones por seguridad.

El núcleo de GNU/Linux proporciona un rango de características internas que le permiten funcionar bastante bien como un cortafuegos de *IP*. La implementación de red incluye código para realizar filtros a nivel de *IP* en numerosas formas, y proporciona un mecanismo para configurar con precisión qué tipos de reglas le gustaría imponer. El cortafuegos en GNU/Linux es suficientemente flexible como para convertirle en algo muy útil en cualquiera de las configuraciones. El Software de cortafuegos de Linux proporciona otras dos características muy útiles que se discutirán en otras secciones: auditoría de *IP* y enmascaramiento de *IP*.

Por otro lado, recordemos los días en los que sólo las grandes compañías se podían permitir disponer de un cierto número de máquinas conectadas por una red local. Frente a aquello, hoy los precios de la tecnología de red han

[100] En Windows, además de interceptar los intentos de acceso desde el exterior también suelen incluir protecciones adicionales contra los troyanos y virus de correo más comunes.

bajado y bajado hasta producir dos consecuencias: La primera, que las redes locales sean algo común, presentes incluso en entornos domésticos. Es seguro que tu tendrás en tu casa dos o más computadoras conectadas por algún tipo de Ethernet. La segunda, que los recursos de red, y de forma especial las direcciones IP, hayan llegado a ser algo escasos y, aunque no están lejanos los tiempos en que eran gratuitos, sean ahora objeto de compraventa.

La mayor parte de la gente que disponga de una *LAN* deseará también disfrutar de una conexión a internet que todas las máquinas de su red puedan utilizar al mismo tiempo. Las reglas del encaminamiento IP son muy estrictas respecto a la forma de manejar esta situación. Las soluciones tradicionales a este problema hubieran pasado por solicitar un conjunto de direcciones *IP*, probablemente un rango de clase C (*192.0.0.0 - 223.255.255.255*), dar a cada máquina de la *LAN* una dirección del rango asignado, y utilizar un enrutador para conectar la *LAN* a internet.

En el actual escenario de una internet mercantilizada, esa solución saldría bastante cara. En primer lugar habría que pagar por el rango de direcciones asignado, en segundo lugar habría que pagar con toda probabilidad al Proveedor de Servicios de internet (*ISP*) por el privilegio de disponer de una ruta hacia la red local en sus máquinas, de tal forma que el resto de internet supiera cómo llegar a ellas. Esto puede sonar posible para algunas empresas, pero en una instalación doméstica los costes no estarían justificados.

Afortunadamente GNU/Linux proporciona una solución al problema, solución que utiliza un componente de un grupo de funcionalidades avanzadas de red llamadas en conjunto Traducción de Direcciones de Red (*NAT*). *NAT* es un conjunto de procedimientos para modificar las direcciones *IP* contenidas en las cabeceras de los datagramas *IP* mientras éstos viajan (al vuelo). Puede sonar extraño, pero mostraremos que se trata de la solución ideal al problema –real para muchos– que acabamos de plantear. '*IP masquerade*' es el nombre que recibe un tipo de traducción de direcciones de red que permite que todas las máquinas de una red privada utilicen internet contando con una única conexión (y una única dirección IP).

El enmascaramiento *IP* (en inglés «*IP masquerading*») permite utilizar un rango de direcciones privadas (reservadas) en la red local y que el encaminador GNU/Linux se encargue de hacer al vuelo ciertas traducciones de direcciones IP y puertos. Cuando le llega un datagrama IP de alguna máquina de la red local, se fija en el protocolo de nivel superior encapsulado en el mismo («*UDP*», «*TCP*», «*ICMP*», etc...) y modifica el datagrama para que parezca que fue generado por el propio encaminador (y re-

cuerda qué ha sido modificado). A continuación saca el datagrama a internet donde aparece generado por la única dirección IP pública del encaminador. Cuando la máquina destino recibe el datagrama cree que se ha originado en la máquina GNU/Linux, y responde a su dirección de internet. Cuando el encaminador GNU/Linux recibe un datagrama en su interfaz de red conectada a internet, busca en su tabla de conexiones enmascaradas en curso para ver si el datagrama pertenece a alguna máquina de la *LAN* y, si es así, deshace la traducción que hizo en el primer datagrama y reenvía este datagrama de respuesta a la máquina local.

Tenemos una pequeña red ethernet en la que utilizamos uno de los rangos de direcciones reservadas. La red dispone de un encaminador con enmascaramiento, una máquina GNU/Linux, por supuesto, que proporciona acceso a internet. Una de las máquinas de la red (192.168.1.3) desea establecer una conexión con el Host remoto 209.1.106.178 en el puerto 8888. El equipo encamina su datagrama por el encaminador con enmascaramiento, que identifica la petición de conexión como requiriente de los servicios de enmascaramiento. El encaminador entonces acepta el datagrama y reserva un número de puerto (1035) para este menester, sustituye la dirección IP y número de puerto de la máquina origen del datagrama por los suyos propios, y transmite el datagrama al Host destino. El Host destino cree que ha recibido una petición de conexión de la máquina GNU/Linux enmascaradora, y genera un datagrama de respuesta. La máquina enmascaradora, al recibir ese datagrama, halla la asociación en su tabla de enmascaramiento y deshace la sustitución que llevó a cabo en el primer datagrama. Entonces transmite el datagrama de respuesta a la máquina origen.

La máquina local cree que se está comunicando directamente con el Host remoto. El Host remoto no sabe nada de la existencia de la máquina local y cree que ha establecido una conexión con la máquina GNU/Linux enmascaradora. La máquina GNU/Linux enmascaradora sabe que las otras dos máquinas están hablando entre sí y en qué puertos, y realiza las traducciones de direcciones y puertos necesarias para que la comunicación tenga lugar.

Efectos Colaterales y Beneficios Accesorios la funcionalidad de enmascaramiento *IP* viene acompañada de su propio conjunto de efectos laterales, algunos son útiles y algunos pueden acabar siendo un problema.

Ninguna de las máquinas en la red detrás del encaminador enmascarador son jamás vistas directamente desde internet. Consecuentemente, solamente

se necesita una dirección *IP* válida y rutable para permitir que todas las máquinas establezcan conexiones hacia internet. Esto tiene un lado no tan bueno: ninguna de esas máquinas es visible desde internet, y por lo tanto no se puede conectar directamente a ellas desde internet. La única máquina visible en una red enmascarada es el propio encaminador enmascarador. Se trata de algo importante cuando se piensa en servicios como el correo o el *FTP*. Resulta de utilidad decidir qué servicios deberían ser provistos por la máquina enmascaradora y para cuáles debería actuar como *Proxy* o tratar de algún otro modo especial.

Segundo, dado que ninguna de las máquinas enmascaradas son visibles, se encuentran relativamente protegidas de ataques del exterior. Eso puede simplificar (o eliminar) la necesidad de puesta a punto de funcionalidades de cortafuegos en la máquina enmascaradora. No se debe confiar demasiado en ésto, puesto que la red local estará únicamente tan segura como lo esté la máquina enmascaradora. Así, si la seguridad es un punto importante, se debería utilizar un cortafuegos para protegerla.

Tercero, el enmascaramiento *IP* tendrá cierto impacto negativo en el rendimiento de su red. En un escenario típico ese impacto negativo será probablemente insignificante. Si se tiene un gran número de sesiones enmascaradas activas puede ocurrir que se perciba cierta sobrecarga en la máquina enmascaradora que afecte negativamente al rendimiento de la red. El enmascaramiento *IP* implica un incremento considerable en el proceso que requiere cada datagrama comparado con el normalmente exigido.

Cuando utilizas un sistema Linux para conectar tu red local a internet, tienes la posibilidad de permitir o no cierto tipo de tráfico. Las cabeceras de los paquetes *IP* contienen información sobre el destino (de forma que se puede prevenir el acceso a ciertos sitios de internet), el origen (se pueden evitar conexiones desde sitios concretos de internet). Otra información que se obtiene de las cabeceras es el protocolo utilizado (*ICMP, UDP, TCP*) y el puerto.

Normalmente los protocolos de alto nivel utilizan para sus conexiones puertos determinados (también llamados *Well Known Sockets*). De esa forma, la mayor parte de las peticiones de documentos html se harán a destinos de internet por el puerto 80, el envío de correo se hará por el puerto 25, o las conexiones vía ssh se harán usando el puerto 22. Para más información ver */etc/services*.

Mediante el proyecto Nftables proporciona filtrado de paquetes y clasificación de paquetes en Linux. Es la evolución de *iptables*, y, de hecho, las

reemplaza (no se puede mezclar *nftables* y *iptables*). *Nftables* es capaz de reemplazar en el mismo Framework a *iptables, ip6tables, arptables y ebtables*, y todo ello bajo el mismo espacio de usuario (nft) y compatibilidad hacia atrás (con sintaxis *iptables*). *Nftables* es el Framework por defecto en Debian GNU/Linux.

Otras opciones de cortafuegos sobre línea de comando son: netfilter, iptables, ufw, apf y shorewall. Y otros con interfaz gráfica son: Gufw, Douane, OpenSnitch entre otros.

10.3 Acceso Remoto Mediante SSH

SSH o Secure Shell[101], es un protocolo de administración remota que permite a los usuarios controlar y modificar equipos de cómputo o servidores de forma remota, a través de internet mediante un mecanismo de autenticación.

Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al servidor y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera cifrada.

Cualquier usuario de Linux, MacOS o Windows[102] puede usar SSH para conectarse a un servidor remoto. Puedes ejecutar comandos Shell de la misma manera que lo harías si estuvieras operando físicamente el equipo remoto.

¿Cómo funciona SSH? si usas Linux o Mac, entonces usar el protocolo SSH es muy fácil. Si utilizas Windows, deberás utilizar un cliente SSH para abrir conexiones SSH. El cliente SSH más popular es PuTTY.

Para usuarios de Mac OS y Linux, debemos abrir el programa de terminal, el comando SSH consta de 3 partes distintas:

```
$ ssh {user}@{Host}[:<puerto>][comando]
```

[101] SSH (o Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

[102] Los usuarios de Windows pueden aprovechar los clientes SSH como Putty.

El comando *ssh* o *mosh*[103] le indica a tu sistema que desea abrir una conexión de Shell Segura y cifrada.

- {user} representa la cuenta a la que deseas acceder. Por ejemplo, puede que quieras acceder al usuario root, que es básicamente para el administrador del sistema con derechos completos para modificar cualquier cosa en el sistema.
- {Host} hace referencia al equipo al que quieres acceder. Esto puede ser una dirección IP (por ejemplo, 244.235.23.19) o un nombre de dominio (por ejemplo, www.xyzdomain.com).
- puerto: Si el puerto de escucha de la máquina remota no es el habitual (el puerto 22) tendremos que especificarlo.

Al pulsar enter, se te pedirá que escribas la contraseña de la cuenta solicitada. Al escribirla, nada aparecerá en la pantalla, pero tu contraseña, de hecho, se está transmitiendo. Una vez que hayas terminado de escribir, pulsa enter una vez más.

Aprendiendo las Diferentes Técnicas de Cifrado La ventaja significativa ofrecida por el protocolo SSH sobre sus predecesores es el uso del cifrado para asegurar la transferencia segura de información entre el Host y el cliente. Host se refiere al servidor remoto al que estás intentando acceder, mientras que el cliente es el equipo que estás utilizando para acceder al Host. Hay tres tecnologías de cifrado diferentes utilizadas por SSH:

- Cifrado simétrico
- Cifrado asimétrico
- Hashing

[103] MOSH (Mobile Shell) como medio de conexión (no corta la comunicación por inactividad como SSH), lo podemos instalar usando:

```
# apt install mosh
```

y su uso es similar al de SSH:

```
$ mosh usuario@192.168.13.230
$ mosh -p 70 usuario@192.168.13.230
```

Cifrado Simétrico es una forma de cifrado en la que se utiliza una clave secreta tanto para el cifrado como para el descifrado de un mensaje, tanto por el cliente como por el Host. Efectivamente, cualquiera que tenga la clave puede descifrar el mensaje que se transfiere.

El cifrado simétrico a menudo se llama clave compartida (shared key) o cifrado secreto compartido. Normalmente sólo hay una clave que se utiliza, o a veces un par de claves donde una clave se puede calcular fácilmente con la otra clave.

Las claves simétricas se utilizan para cifrar toda la comunicación durante una sesión SSH. Tanto el cliente como el servidor derivan la clave secreta utilizando un método acordado, y la clave resultante nunca se revela a terceros. El proceso de creación de una clave simétrica se lleva a cabo mediante un algoritmo de intercambio de claves.

Lo que hace que este algoritmo sea particularmente seguro es el hecho de que la clave nunca se transmite entre el cliente y el Host. En lugar de eso, los dos equipos comparten datos públicos y luego los manipulan para calcular de forma independiente la clave secreta. Incluso si otra máquina captura los datos públicamente compartidos, no será capaz de calcular la clave porque el algoritmo de intercambio de clave no se conoce.

Debe tenerse en cuenta, sin embargo, que el token secreto es específico para cada sesión SSH, y se genera antes de la autenticación del cliente. Una vez generada la clave, todos los paquetes que se mueven entre las dos máquinas deben ser cifrados por la clave privada. Esto incluye la contraseña escrita en la consola por el usuario, por lo que las credenciales siempre están protegidas de los fisgones de paquetes de red.

Existen varios códigos cifrados simétricos, incluyendo, pero no limitado a, AES (Advanced Encryption Standard), CAST128, Blowfish, etc. Antes de establecer una conexión segura, el cliente y un Host deciden qué cifrado usar, publicando una lista de cifrados soportados por orden de preferencia. El cifrado preferido de entre los soportados por los clientes que está presente en la lista del Host se utiliza como el cifrado bidireccional.

Cifrado Asimétrico a diferencia del cifrado simétrico, el cifrado asimétrico utiliza dos claves separadas para el cifrado y el descifrado. Estas dos claves se conocen como la clave pública (public key) y la clave privada (private key). Juntas, estas claves forman el par de claves pública-privada (public-private key pair).

La clave pública, como sugiere el nombre, se distribuye abiertamente y se comparte con todas las partes. Si bien está estrechamente vinculado con la clave privada en términos de funcionalidad, la clave privada no se puede calcular matemáticamente desde la clave pública. La relación entre las dos claves es altamente compleja: un mensaje cifrado por la clave pública de una máquina, sólo puede ser descifrado por la misma clave privada de la máquina. Esta relación unidireccional significa que la clave pública no puede descifrar sus propios mensajes ni descifrar nada cifrado por la clave privada.

La clave privada debe permanecer privada, es decir, para que la conexión sea asegura, ningún tercero debe conocerla. La fuerza de toda la conexión reside en el hecho de que la clave privada nunca se revela, ya que es el único componente capaz de descifrar mensajes que fueron cifrados usando su propia clave pública. Por lo tanto, cualquier parte con la capacidad de descifrar mensajes firmados públicamente debe poseer la clave privada correspondiente.

A diferencia de la percepción general, el cifrado asimétrico no se utiliza para cifrar toda la sesión SSH. En lugar de eso, sólo se utiliza durante el algoritmo de intercambio de claves de cifrado simétrico. Antes de iniciar una conexión segura, ambas partes generan pares de claves públicas-privadas temporales y comparten sus respectivas claves privadas para producir la clave secreta compartida.

Una vez que se ha establecido una comunicación simétrica segura, el servidor utiliza la clave pública de los clientes para generar y desafiar y transmitirla al cliente para su autenticación. Si el cliente puede descifrar correctamente el mensaje, significa que contiene la clave privada necesaria para la conexión. Y entonces comienza la sesión SSH.

Hashing el hashing unidireccional es otra forma de criptografía utilizada en Secure Shell Connections. Las funciones de hash unidireccionales difieren de las dos formas anteriores de cifrado en el sentido de que nunca están destinadas a ser descifradas. Generan un valor único de una longitud fija para cada entrada que no muestra una tendencia clara que pueda explotarse. Esto los hace prácticamente imposibles de revertir.

Es fácil generar un hash criptográfico de una entrada dada, pero imposible de generar la entrada del hash. Esto significa que si un cliente tiene la entrada correcta, pueden generar el hash criptográfico y comparar su valor para verificar si poseen la entrada correcta.

SSH utiliza hashes para verificar la autenticidad de los mensajes. Esto se hace usando HMACs, o códigos de autenticación de mensajes basados en hash. Esto asegura que el comando recibido no se altere de ninguna manera.

Mientras se selecciona el algoritmo de cifrado simétrico, también se selecciona un algoritmo de autenticación de mensajes adecuado. Esto funciona de manera similar a cómo se selecciona el cifrado, como se explica en la sección de cifrado simétrico.

Todo mensaje transmitido debe contener un MAC, que se calcula utilizando la clave simétrica, el número de secuencia de paquetes y el contenido del mensaje. Se envía fuera de los datos cifrados simétricamente como la sección final del paquete de comunicaciones.

¿Cómo Funciona el Protocolo SSH con estas Técnicas de Cifrado? la forma en que funciona SSH es mediante el uso de un modelo cliente-servidor para permitir la autenticación de dos sistemas remotos y el cifrado de los datos que pasa entre ellos.

SSH opera en el puerto TCP 22 de forma predeterminada (aunque esto se puede cambiar si es necesario). El Host (servidor) escucha en el puerto 22 (o cualquier otro puerto SSH asignado) para las conexiones entrantes. Organiza la conexión segura mediante la autenticación del cliente y la apertura del entorno de Shell correcto si la verificación tiene éxito.

El cliente debe iniciar la conexión SSH iniciando el protocolo TCP con el servidor, asegurando una conexión simétrica segura, verificando si la identidad mostrada por el servidor coincide con los registros anteriores (normalmente grabados en un archivo de almacén de claves RSA) y presenta las credenciales de usuario necesarias para autenticar la conexión.

Hay dos etapas para establecer una conexión: primero ambos sistemas deben acordar estándares de cifrado para proteger futuras comunicaciones, y segundo, el usuario debe autenticarse. Si las credenciales coinciden, se concede acceso al usuario.

Negociación de Cifrado de Sesión cuando un cliente intenta conectarse al servidor a través de TCP, el servidor presenta los protocolos de cifrado y las versiones respectivas que soporta. Si el cliente tiene un par similar de protocolo y versión, se alcanza un acuerdo y se inicia la conexión con el protocolo aceptado. El servidor también utiliza una clave pública asimétrica que el cliente puede utilizar para verificar la autenticidad del Host.

Una vez que esto se establece, las dos partes usan lo que se conoce como Algoritmo de Intercambio de Claves Diffie-Hellman para crear una clave simétrica. Este algoritmo permite que tanto el cliente como el servidor lleguen a una clave de cifrado compartida que se utilizará en adelante para cifrar toda la sesión de comunicación.

Aquí es cómo el algoritmo trabaja en un nivel muy básico:

1. Tanto el cliente como el servidor coinciden en un número primo muy grande, que por supuesto no tiene ningún factor en común. Este valor de número primo también se conoce como el valor semilla (seed value).

2. Luego, las dos partes acuerdan un mecanismo de cifrado común para generar otro conjunto de valores manipulando los valores semilla de una manera algorítmica específica. Estos mecanismos, también conocidos como generadores de cifrado, realizan grandes operaciones sobre la semilla. Un ejemplo de dicho generador es AES (Advanced Encryption Standard).

3. Ambas partes generan independientemente otro número primo. Esto se utiliza como una clave privada secreta para la interacción.

4. Esta clave privada recién generada, con el número compartido y el algoritmo de cifrado (por ejemplo, AES), se utiliza para calcular una clave pública que se distribuye a la otra computadora.

5. A continuación, las partes utilizan su clave privada personal, la clave pública compartida de la otra máquina y el número primo original para crear una clave compartida final. Esta clave se calcula de forma independiente por ambos equipos, pero creará la misma clave de cifrado en ambos lados.

6. Ahora que ambas partes tienen una clave compartida, pueden cifrar simétricamente toda la sesión SSH. La misma clave se puede utilizar para cifrar y descifrar mensajes (leer: sección sobre cifrado simétrico).

Ahora que se ha establecido la sesión cifrada segura simétricamente, el usuario debe ser autenticado.

Instalación de OpenSSH y Puesta en Marcha OpenSSH es el programa servidor/cliente SSH más utilizado por los Routers, Switches, servidores y un largo etcétera de dispositivos. Este programa es completamente gratuito y de código abierto. La instalación de este servidor SSH (si es que no lo tienes ya instalado por defecto) es muy sencilla, simplemente debemos poner en un terminal la siguiente orden:

```
# apt install openssh-server
```

una vez instalado, estamos listos para que nuestro equipo -ahora ya es un servidor- reciba usuarios remotos.

10.4 Copiar Archivos Entre Equipos

scp permite transferir archivos y/o directorios de una máquina a otra de forma cifrada usando *SSH* (Secure Shell) que es un protocolo de administración remota que le permite al usuario controlar y modificar servidores remotos a través de un mecanismo de autentificación[104]. El comando *scp* (Secure Copy Protocol) tiene una sintaxis similar al del comando *cp*, con la salvedad que es necesario indicar el usuario, la máquina y el subdirectorio de trabajo del archivo y/o directorio para el destino, fuente o ambos.

Por ejemplo, si se desea transmitir un archivo a una máquina *192.168.13.230* con usuario *antonio*, en el directorio *~/Datos/* estando en sesión en otra máquina, se usa la siguiente sintaxis:

```
$ scp archivo.dat antonio@192.168.13.230:~/Datos/
```

Si se desea transmitir un subdirectorio a la máquina *192.168.13.230*, en el directorio *home* del usuario (denotado con .), se usa la siguiente sintaxis:

```
$ scp -r Directorio antonio@192.168.13.230:.
```

también podemos decirle que excluya algunos archivos (*.mp3) de la copia, usando:

```
$ scp -r !(*.mp3) Directorio antonio@192.168.13.230:.
```

[104] En Android podemos hacer uso de SSH/SFTP mediante aplicaciones como: Termius, JuiceSSH, Mobile SSH, Advanced Client app, ConnectBot.

Si se desea copiar un archivo de una máquina remota a nuestra máquina, usamos:

```
$ scp antonio@192.168.13.230:~/archivo ~/destino/
```

o de forma alternativa usamos (. indica el directorio donde el usuario se encuentra):

```
$ scp antonio@192.168.13.230:~/archivo .
```

Si se desea copiar de una máquina remota a otra máquina remota, usamos:

```
$ scp user1@HOST1:~/archivo user2@HOST2:~/
```

Si se desea transferir míltiples archivos podemos usar:

```
$ scp file1.txt file2.txt user@HOST:/home/user/
```

o de forma alternativa usamos (. indica el directorio donde el usuario se encuentra):

```
$ scp user@Host:/home/user/\{file1.txt,file2.txt\} .
```

En el caso que se quiera limitar el ancho de banda en la transmisión de archivos por *scp*, usar:

```
$ scp -l 400 user@server:/home/user/* .
```

En el caso de que se desee usar otro puerto distinto al de imisión (22) usar:

```
$ scp -P 4455 file.txt user@HOST:/home/user/file.txt
```

En el caso de querer incrementar la velocidad de transferencia en el uso de *scp*, la opción más viable es el cambiar el cifrado usada por omisión por otras como *3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes-128-ctr, aes192-ctr, eas256-ctr, arcfour256, arcfour, blowfish-cbc y cast128-cbc* mediante:

```
$ scp -c blowfish user@server:/home/user/file .
```

o de forma alternativa usamos:

```
$ scp -c arcfour256 user@HOST:/home/user/file .
```

Si adicionalmente se quiere compactar para reducir el tiempo de transferencia, usamos:

```
$ scp -C SourceFile user@HOST:/home/user/TargetFile
```

Si se desea que no se muestre información de la transferencia de los archivos al usar *scp* usar:

```
$ scp -q SourceFile user@HOST:/home/user/TargetFile
```

o si desea ver más información en la transferencia usar:

```
$ scp -v SourceFile user@HOST:/home/user/TargetFile
```

Si se instala *sshpass*, entonces hacemos:

```
$ sshpass -p "your_password" scp -r backup_user@target_ip:/home/
/backup/$name
```

rsync es una aplicación libre y multiplataforma que ofrece transmisión eficiente de datos incrementales, que opera también con datos comprimidos y cifrados. Mediante una técnica de Delta Encoding, que permite sincronizar archivos y directorios entre dos máquinas de una red o entre dos ubicaciones en una misma máquina, minimizando el volumen de datos transferidos. Es ideal para trabaja en varias máquinas en las que se desea tener sincronizada una o más carpetas, para instalar usamos:

```
# apt install rsync
```

La sintaxis básica es:

$ rsync [Opciones[105]] Origen [Origen]... Destino

por ejemplo, para hacer la sincronización de la carpeta ~/*Datos* a ~/*Respaldo* usamos:

$ rsync ~/Datos/ ~/Respaldo/

Si queremos saber que hará el comando pero sin hacer la operación indicada, podemos usar la opción –dry-run, por ejemplo:

$ rsync –dry-run ~/Datos/ ~/Respaldo/

hay varias opciones que podemos usar en *rsync*, ejemplo de ellas es:

$ rsync –verbose –recursive –links –hard-links –times –delete –stats ~/Datos/ ~/Respaldo/

en este caso se sincronizaría el contenido de ~/Datos con ~/*Respaldo*, pero lo hará mostrando lo que transfiere, de forma recursiva, conservará enlaces simbólicos y sus tiempos, borrará los archivos que estén en el destino pero no en el origen y al terminar mostrará las estadísticas de la transferencia.

Para hacer la transmisión cifrada entre equipos, podemos usar *rsync* conjuntamente con *ssh*, supongamos que se esta en la máquina y quiere tener sincronizada la carpeta ~/Datos con mas de un equipo, mediante *ssh* usando un puerto *343*, en la máquina *192.168.13.230* y usuario *antonio*, usar:

$ rsync –partial –recursive –links –hard-links –times –verbose –delete –stats ~/Datos/ -e 'ssh -p 343' antonio@192.168.13.230: ~/Respaldo/

por supuesto esto puede hacerse en cualquier dirección, i.e. de la máquina remota a nuestra máquina o viceversa, ejemplo:

$ rsync –partial –recursive –links –hard-links –times –verbose –delete –stats -e 'ssh -p 343' antonio@192.168.13.230: ~/Respaldo/ ~/Datos/

[105] Algunas opciones son: -r recursivo, -b backups, -R relativo, -u actualiza, -p muestra el progreso, -c comprime, -p preserva permisos, -v muestra lo que hace, -q trabaja en modo silencioso, -l preserva ligas simbólicas, -H preserva enlaces duros, -t preserva tiempos de modificación, etc.

pssh permite transferir o copiar archivos a múltiples servidores en Linux con un mismo comando:

- pscp - es una utilería para copiar archivos en paralelo a múltiples equipos
- prsync - es una utilería para transferir de forma eficiente archivos entre múltiples equipos en paralelo
- pnuke - permite concluir procesos en múltiples equipos en paralelo
- pslurp - permite copiar archivos de múltiples equipos a un equipo central en paralelo

Si creamos un archivo *Hosts.txt*, con los *IPs* como el siguiente:

192.168.0.3:22
192.168.0.9:22

podemos usar para copiar un archivo a múltiples servidores:

$ pscp -h Hosts.txt -l USR -Av wine-1.7.55.tar.bz2 /tmp/

o de forma alternativa usamos:

$ pscp.pssh -h Hosts.txt -l USR -Av wine-1.7.55.tar.bz2 /tmp/

donde:

-h indica que se lean los *IPs* del archivo indicado
-l se indica el usuario a usar en todos los equipos.
-A solicita el password para ser enviado a *ssh*
-v visualiza las operaciones y mensajes que genera el comando

Podemos copiar directorios a múltiples servidores, usando:

$ pscp -h myscpHosts.txt -l USR -Av -r Android\ Games/ /tmp/

o de forma alternativa:

$ pscp.pssh -h myscpHosts.txt -l USR -Av -r Android\ Games/ /tmp/

nc el comando *netcat* (*nc*) es una utilidad que permite escribir y leer datos a través de conexiones de red usando los protocolos TCP y UDP. Supongamos que estamos en el IP 192.168.13.230. Podemos generar un archivo compactado, cifrarlo y enviarlo a otro equipo en una mismo comando mediante:

```
$ tar -cvzf - directorio | gpg -c | nc -l 6666
```

y para recibirlo en el otro equipo usamos:

```
$ nc 192.168.13.230 6666 | gpg -d | tar -xvzf -
```

Siempre es mejor opción usar *scp*, pero *nc* cumplirá con su cometido.

11 Apéndice A: Software Libre y Propietario

Con el constante aumento de la comercialización de equipos de cómputo y/o comunicación (teléfonos inteligentes, tabletas, computadoras portátiles y de escritorio, etc.) y su relativo bajo costo, estos equipos se han convertido en objetos omnipresentes en nuestra vida diaria, ya que estos permiten realizar un creciente número de actividades cotidianas de miles de millones de usuarios.

Dichos equipos de cómputo y/o comunicación por sí solos tienen poca utilidad, pero su uso en conjunción con el Software adecuado forman un dúo que nos ha permitido tener los avances de los que actualmente disfrutamos. El Software -sistema operativo y los programas de aplicaciones- son los que realmente generan las soluciones al interactuar uno o más paquetes informáticos con los datos del usuario. También, es común que al comprar un equipo de cómputo y/o comunicación, en el costo total, se integre el del sistema operativo, aplicaciones ofimáticas y de antivirus, sean estos usados por el usuario o no y en la mayoría de los casos no es posible solicitar que no sean incluidos en el costo del equipo.

Por otro lado, el Software comercial suele quedar obsoleto muy rápido, ya que constantemente se le agregan nuevas funcionalidades al mismo y estas en general son vendidas como versiones independientes de la adquirida originalmente. Esto obliga al usuario -si quiere hacer uso de ellas- a comprar las nuevas versiones del Software para satisfacer sus crecientes necesidades informáticas y la obsolescencia programada.

Por lo anterior y dada la creciente complejidad de los paquetes de cómputo y el alto costo de desarrollo de aplicaciones innovadoras, en muchos casos, el costo total del Software que comúnmente los usuarios instalan -y que no necesariamente usan las capacidades avanzadas del programa, por las cuales el Software tiene un alto costo comercial- en sus equipos, suele ser más caro que el propio equipo en el que se ejecutan.

Hoy en día los usuarios disponemos de dos grandes opciones para adquirir el Software necesario para que nuestros equipos funcionen, a saber:

- Por un lado, podemos emplear programas comerciales (Software propietario), de los cuales no somos dueños del Software, sólo concesionarios al adquirir una licencia de uso del Software y nos proporcionan un instalable del programa adquirido. La licencia respectiva es en la gran mayoría de los casos muy restrictiva, ya que restringe su uso a un solo

equipo y/o usuario simultáneamente.

- Por otro lado, existe el Software libre[106], desarrollado por usuarios y para usuarios que, entre otras cosas, comparten los códigos fuente, el programa ejecutable y dan libertades para estudiar, adaptar y redistribuir a quien así lo requiera el programa y todos sus derivados.

Sobre la Obsolescencia Programada Es un conjunto de estrategias deliberadas destinadas a asegurarse que la versión actual de un determinado producto quedará desfasada o inservible en un plazo de tiempo predeterminado. De esta manera, los fabricantes se aseguran que los consumidores se verán obligados a reemplazarlo aunque funcione adecuadamente.

La obsolescencia puede lograrse mediante la introducción de un modelo con características superiores o diseñando intencionadamente un producto para que deje de funcionar correctamente en un plazo determinado. En cualquiera de los dos casos, se espera que los consumidores opten por el nuevo producto de la misma marca. Muchas veces la obsolescencia no es sobre el propio producto sino aplicando restricciones al producto de un competidor con la ayuda de una tercera empresa.

Tipos de Obsolescencia Programada Podemos dividir la obsolescencia programada en 4 tipos:

1- Establecimiento artificial del plazo de duración: Los productos se fabrican con piezas cuya duración tienen una vida útil limitada cuando, si se usaran otras de calidad superior ese plazo se extendería.

2- Actualizaciones de Software: Los desarrolladores de Software sacan nuevas versiones de sus aplicaciones que en un momento determinado dejan de ser compatibles con dispositivos antiguos. En muchos casos se ha podido comprobar que esa incompatibilidad es absolutamente artificial ya que al «engañar» al Software este funcionaba sin problemas.

[106] A veces también se han usado términos como FOSS y FLOSS. Ambas cosas son similares, ya que FOSS (Free and Open Source Software) traducido como "Software de código abierto" y FLOSS (Free/Libre and Open Source Software) "Software libre y de código abierto". Según quienes adoptan estos términos, lo hacen por tener una imparcialidad entre la carga filosófica del Software libre y el aspecto técnico y/o las ventajas que brinda este modelo de desarrollo. Richard Stallman nos invita a no usarlas y no se trata de un ad hóminem. Stallman y el proyecto GNU nos aconsejan que hablemos siempre de Software libre y aquí no cabe imparcialidad.

3- Obsolescencia percibida: Esta es una táctica psicológica, se trata de convencer al consumidor mediante publicidad y el uso de influenciadores de que el producto que se tiene actualmente está viejo y que se necesita uno nuevo. Como por ejemplo: ¿cuantos megapíxeles necesitas en tu teléfono para sacar una buena foto de tu mascota?

4- Trabas a la reparación: En el caso de los teléfonos por ejemplo, lo de impedir sacar la batería (con la excusa de hacer los teléfonos más delgados) es una forma de obligar a los consumidores a recurrir a los servicios oficiales y a disuadirlos de reemplazarlas por sustitutos más económicos. Otras tácticas son la utilización de piezas no estándar o que necesitan herramientas específicas para la reparación. Muchas veces se suele restringir el acceso a estas piezas o hacer una reducida producción de las mismas para aumentar artificialmente el costo.

Ejemplos de Obsolescencia Programada

- iPhone cada vez más lentos: La Justicia francesa comprobó que actualizaciones de Software hacían cada vez más lento el rendimiento de los modelos más viejos. La empresa le echó la culpa a las baterías, pero pagó una compensación de decenas de millones de dólares. Además rebajó los precios de sus baterías de repuesto para que los teléfonos fueran más rápidos con el nuevo Software y se comprometió a hacer más en el futuro para garantizar que los teléfonos no volvieran a ser más lentos. Con la salida de un nuevo modelo de teléfono cada año, seguro que hay algo de obsolescencia planificada en alguna parte.

- Impresoras: Esto es algo que todos conocemos. Muchas veces nos encontramos con impresoras a precio rebajado, pero al momento de tener que comprar un cartucho de tinta nos encontramos con que este tiene un precio igual o superior a comprar una nueva. Además, se ponen restricciones a la recarga o al uso de cartuchos alternativos. Hubo denuncias de que algunos modelos dejaban de funcionar a partir de cierta cantidad de páginas impresas o cierto tiempo desde la primera impresión.

- Certificados de seguridad: Por ejemplo, el pasado 30 de septiembre de 2021 caduco otro certificado de autentificación (CA de DST Root CA X3 de Let's Encrypt) que ayudaba a validar la conexión en internet a

los dispositivos que no fueron actualizados a otro certificado más actual -en la mayoría de los casos por no ser del interés económico de sus creadores-. Esto ocasionó que millones de dispositivos (teléfonos inteligentes, Smart TV, tabletas, computadoras portátiles y de escritorio, etc.) con algunos años de ser creados y perfectamente funcionales dejarán de conectarse a internet de un día para otro, forzando a sus dueños a desechar el dispositivo por carecer del servicio de internet en las aplicaciones instaladas.

- Cambio de la versión del sistema operativo: En el caso del sistema operativo Windows 10 a 11, la solicitud de requisitos mínimos de Hardware es para muchos equipos excesivo, ya que se estima que dejará fuera en su actualización a casi todos los equipos con más de 4 años de antigüedad por no contar por ejemplo con el Chip TPM 2.0 o GPU compatible con DirectX 12, siendo perfectamente funcionales con la versión actual del sistema operativo. Si bien Windows 10 seguirá con soporte hasta 2025, los usuarios que deseen tener las nuevas características del sistema operativo tendrán que cambiar de equipo.

11.1 Software Propietario

No existe consenso sobre el término a utilizar para referirse al opuesto del Software libre. La expresión «Software propietario (Proprietary Software)» (véase [10]), en la lengua anglosajona, "Proprietary" significa «poseído o controlado privadamente (Privately Owned and Controlled)», que destaca la manutención de la reserva de derechos sobre el uso, modificación o redistribución del Software. Inicialmente utilizado, pero con el inconveniente de que la acepción proviene de una traducción literal del inglés, no correspondiendo su uso como adjetivo en el español, de manera que puede ser considerado como un barbarismo.

El término "propietario" en español resultaría inadecuado, pues significa que «tiene derecho de propiedad sobre una cosa», por lo que no podría calificarse de "propietario" al Software, porque éste no tiene propiedad sobre nada (es decir, no es dueño de nada) y además, no podría serlo (porque es una cosa y no una persona). Así mismo, la expresión "Software propietario" podría ser interpretada como: "Software sujeto a propiedad" (derechos o titularidad) y su opuesto, el Software libre, también está sujeto al derecho de autor. Otra interpretación es que contrariamente al uso popular del término, se puede

afirmar que "todo Software es propietario", por lo que la forma correcta de referirse al Software con restricciones de uso, estudio, copia o mejora es la de Software privativo, según esta interpretación el término "propietario" podría aplicarse tanto para Software libre como Software privativo, ya que la diferencia entre uno y otro está en que el dueño del Software privativo lo licencia como propiedad privada y el de Software libre como propiedad social.

Con la intención de corregir el defecto de la expresión "Software propietario" aparece el llamado "Software con propietario", sin embargo se argumenta contra el término "con propietario" y justamente su similitud con Proprietary en inglés, que sólo haría referencia a un aspecto del Software que no es libre, manteniendo una de las principales críticas a éste (de "Software sujeto a derechos" o "propiedad"). Adicionalmente, si "propietario" se refiere al titular de los derechos de autor -y está claro que no se puede referir al usuario, en tanto éste es simplemente un cesionario-, no resuelve la contradicción: todo el Software libre tiene también titulares de derechos de autor.

La expresión Software no libre (en inglés Non-Free Software) es usado por la FSF para agrupar todo el Software que no es libre, es decir, incluye al llamado en inglés "Semi-Free Software" (Software semilibre) y al "Propietary Software". Asimismo, es frecuentemente utilizado para referirse al Software que no cumple con las Directrices de Software libre de Debian GNU/Linux, las cuales siguen la misma idea básica de libertad en el Software, propugnada por la FSF y sobre las cuales está basada la definición de código abierto de la Open Source Initiative.

Adicionalmente el Software de código cerrado nace como antónimo de Software de código abierto y por lo tanto se centra más en el aspecto de ausencia de acceso al código que en los derechos sobre el mismo, éste se refiere sólo a la ausencia de una sola libertad por lo que su uso debe enfocarse sólo a este tipo de Software y aunque siempre signifique que es un Software que no es libre, no tiene que ser Software de código cerrado.

La expresión Software privado es usada por la relación entre los conceptos de tener y ser privado. Este término sería inadecuado debido a que, en una de sus acepciones, la palabra "privado" se entiende como antónimo de "público", es decir, que «no es de propiedad pública o estatal, sino que pertenece a particulares», provocando que esta categoría se interpretará como no referente al Estado, lo que produciría la exclusión del Software no libre generado por el aparato estatal. Además, el "Software público" se asocia generalmente con Software de dominio público.

11.2 Software Libre

La definición de Software libre (véase [12], [13], [8], [9], [7] y [11]) estipula los criterios que se tienen que cumplir para que un programa sea considerado libre. De vez en cuando se modifica esta definición para clarificarla o para resolver problemas sobre cuestiones delicadas. «Software libre» significa que el Software respeta la libertad de los usuarios y la comunidad. En términos generales, los usuarios tienen la libertad de copiar, distribuir, estudiar, modificar y mejorar el Software. Con estas libertades, los usuarios -tanto individualmente como en forma colectiva- controlan el programa y lo que hace.

Cuando los usuarios no controlan el programa, el programa controla a los usuarios. Los programadores controlan el programa y a través del programa, controlan a los usuarios. Un programa que no es libre, llamado «privativo o propietario», es considerado por muchos como un instrumento de poder injusto.

El Software libre es la denominación del Software que respeta la libertad de todos los usuarios que adquirieron el producto y por tanto, una vez obtenido el mismo puede ser usado, copiado, estudiado, modificado y redistribuido libremente de varias formas. Según la Free Software Foundation (véase [12]), el Software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir y estudiar el mismo, e incluso modificar el Software y distribuirlo modificado.

Un programa es Software libre si los usuarios tienen las cuatro libertades esenciales:

0. La libertad de usar el programa, con cualquier propósito.

1. La libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a tus necesidades.

2. La libertad de distribuir copias del programa, con lo cual puedes ayudar a tu prójimo.

3. La libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie.

Un programa es Software libre si los usuarios tienen todas esas libertades. Por tanto, el usuario debe ser libre de redistribuir copias, tanto con o sin modificaciones, ya sea gratuitamente o cobrando una tarifa por la distribución,

a cualquiera en cualquier parte. El ser libre de hacer estas cosas significa, entre otras cosas, que no tiene que pedir ni pagar el permiso.

También debe tener la libertad de hacer modificaciones y usarlas en privado para su propio trabajo o pasatiempo, sin siquiera mencionar que existen. Si publica sus cambios, no debe estar obligado a notificarlo a nadie en particular, ni de ninguna manera.

La libertad de ejecutar el programa significa que cualquier tipo de persona u organización es libre de usarlo en cualquier tipo de sistema de computación, para cualquier tipo de trabajo y finalidad, sin que exista obligación alguna de comunicarlo al programador ni a ninguna otra entidad específica. En esta libertad, lo que importa es el propósito de los usuarios, no el de los programadores. El usuario es libre de ejecutar el programa para alcanzar sus propósitos y si lo distribuye a otra persona, también esa persona será libre de ejecutarlo para lo que necesite; nadie tiene derecho a imponer sus propios objetivos.

La libertad de redistribuir copias debe incluir las formas binarias o ejecutables del programa, así como el código fuente, tanto para las versiones modificadas como para las que no lo estén. Distribuir programas en forma de ejecutables es necesario para que los sistemas operativos libres se puedan instalar fácilmente. Resulta aceptable si no existe un modo de producir un formato binario o ejecutable para un programa específico, dado que algunos lenguajes no incorporan esa característica, pero debe tener la libertad de redistribuir dichos formatos si encontrara o programara una forma de hacerlo.

Para que se de la libertad que se menciona en los puntos 1 y 3 de realizar cambios y publicar las versiones modificadas tenga sentido, el usuario debe tener acceso al código fuente del programa. Por consiguiente, el acceso al código fuente es una condición necesaria para el Software libre. El «código fuente» compilado no es código fuente real y no cuenta como código fuente.

La libertad 1 incluye la libertad de usar su versión modificada en lugar de la original. Si el programa se entrega con un producto diseñado para ejecutar versiones modificadas de terceros, pero rechaza ejecutar las suyas, una práctica conocida como «tivoización» o «arranque seguro» [«Lockdown»] la libertad 1 se convierte más en una ficción teórica que en una libertad práctica, esto no es suficiente, en otras palabras, estos binarios no son Software libre, incluso si se compilaron desde un código fuente que es libre.

Una manera importante de modificar el programa es agregándole subrutinas y módulos libres ya disponibles. Si la licencia del programa especifica que no se pueden añadir módulos que ya existen y que están bajo una licencia

apropiada, por ejemplo si requiere que usted sea el titular de los derechos de autor del código que desea añadir, entonces se trata de una licencia demasiado restrictiva como para considerarla libre.

La libertad 3 incluye la libertad de publicar sus versiones modificadas como Software libre. Una licencia libre también puede permitir otras formas de publicarlas; en otras palabras, no tiene que ser una licencia de Copyleft. No obstante, una licencia que requiera que las versiones modificadas no sean libres, no se puede considerar libre.

«Software libre» no significa que «no es comercial». Un programa libre debe estar disponible para el uso comercial, la programación comercial y la distribución comercial. La programación comercial de Software libre ya no es inusual; el Software libre comercial es muy importante, ejemplo de ello es la empresa RedHat (ahora propiedad de IBM). Puede haber pagado dinero para obtener copias de Software libre, o puede haber obtenido copias sin costo. Pero sin tener en cuenta cómo obtuvo sus copias, siempre tiene la libertad de copiar y modificar el Software, incluso de vender copias.

El término Software no libre se emplea para referirse al Software distribuido bajo una licencia de Software más restrictiva que no garantiza estas cuatro libertades. Las leyes de la propiedad intelectual reservan la mayoría de los derechos de modificación, duplicación y redistribución para el dueño del Copyright; el Software dispuesto bajo una licencia de Software libre rescinde específicamente la mayoría de estos derechos reservados.

Los manuales de Software deben ser libres por las mismas razones que el Software debe ser libre y porque de hecho los manuales son parte del Software. También tiene sentido aplicar los mismos argumentos a otros tipos de obras de uso práctico, es decir, obras que incorporen conocimiento útil, tal como publicaciones educativas y de referencia. Wikipedia es el ejemplo más conocido.

La lista de proyectos de este tipo es realmente impresionante, algunos han conseguido un uso y alta calidad, por ejemplo el compilador GCC, el Kernel de Linux y el sistema operativo Debian GNU/Linux y Android. Mientras que otros proyectos han caído en el olvido, pero de la gran mayoría se tiene copia del código fuente que permitiría a quienes estén interesados en dicho proyecto poder reusarlo y en su caso ampliarlo.

La característica más importante que aparece típicamente en un proyecto de este tipo, es que un conjunto de personas separadas a gran distancia, sean capaces, a través de la Web, de los E-mail y de foros de aunar sus esfuerzos para crear, mejorar y distribuir un producto, de forma que todos

ellos se benefician unos de otros. Evidentemente, la mayor parte del peso recae en los desarrolladores, pero también es necesaria una difusión para que los usuarios documenten, encuentren errores, hagan foros de discusión, etc.

Si bien, el Software libre no es más seguro (en el sentido de invulnerable) que el propietario, la diferencia estriba en que el código fuente en el Software libre está disponible para todos y cualquiera puede aportar una solución, y por lo general al poco tiempo de detectarse una vulnerabilidad (a veces en cuestión de horas) se puede disponer de una solución para la misma. Además, al tener acceso al código fuente se puede detectar fácilmente si alguien introdujo código malicioso a una determinada aplicación.

¿Por qué se Interesan los Autores, Alumnos y Profesores Universitarios en el Software Libre? La ventaja principal es porque bajo el Software libre subyace la idea de compartir conocimiento y favorecer la existencia de nuevas ideas[107]; y ¿qué es investigar y enseñar?, sino crear conocimiento y procurar que los alumnos aprendan e incluso vayan más allá de lo aprendido. Se comparte la idea, que el espíritu del Software libre es similar al que debería reinar en las instituciones educativas:

- Porque así no se condiciona a los estudiantes a usar siempre lo mismo.
- No se fomenta la piratería en los estudiantes y se evita pagar licencias que no son necesarias al existir alternativas gratuitas.
- Es mucho más seguro ya que el Software libre es público y se puede ver qué hace exactamente sin recelos.
- Se ofrece libertad de elección a los estudiantes y profesores al no limitarlos a usar una solución determinada, ampliando sus opciones y permitiendo un mayor aprendizaje.

Concretando estas ideas, profesores e investigadores necesitan herramientas para la investigación y docencia y estas deben tener una calidad mínima y ser fácilmente distribuibles entre los alumnos. En muchos casos las compañías desarrolladoras y distribuidoras de programas de cómputo no han

[107] ¿Por qué el Software creado con dinero de los impuestos no se publica como Software Libre?

¡El código pagado por los ciudadanos debería estar disponible para los ciudadanos y el mismo gobierno!

sabido ofrecer sus productos con la flexibilidad adecuada para las labores docentes o, en otros casos, los productos desarrollados no tienen la calidad esperada.

El Software libre es aún joven, pese a las decenas de miles de proyectos actuales -en los que se trabaja constantemente en mejorar la parte computacional de los algoritmos involucrados en el proyecto, haciendo y puliendo interfaces gráficas, generando ayuda en línea así como la documentación necesaria para que usuarios noveles y avanzados usen la mayor cantidad de opciones programadas- existen muchas otras necesidades profesionales y de investigación que requieren el desarrollo innovador de programas de cómputo para automatizarlas y hacerlas eficientes. Esto queda plasmado en las decenas de proyectos que a diario son registrados en las páginas especializadas en busca de difusión y apoyo para su proyecto.

En los últimos años, muchos proyectos han pasado de ser simples programas en línea de comandos a complejas aplicaciones multiplataforma -se ejecutan en distintos sistemas operativos como son Windows, Linux, Unix, Mac OS, Android- con ambientes gráficos multimedia que en muchos casos han superado a sus contrapartes comerciales -por ejemplo los navegadores Web-. Para muestra de este maravilloso avance, tomemos el proyecto del sistema operativo Android, que actualmente se ejecuta en millones de equipos -como celulares, tabletas, electrodomésticos, etc.- y en los cuales se pueden descargar miles de aplicaciones y está soportado por una gran cantidad de usuarios y empresas comerciales como Google, IBM y últimamente Microsoft -que años atrás era acérrima enemiga del Software libre-.

El Software libre ha logrado desplazar a muchos de sus competidores por sus múltiples bondades y bajo costo de desarrollo -es el caso de Windows Phone que fue reemplazado por Android de Google-, al reusar miles de aplicaciones ya existentes que usan Software libre y permitir desarrollar otro tanto de aplicaciones bajo una plataforma que se ejecuta en los más diversos procesadores. Además, el uso de Software libre y su posibilidad de ampliarlo y/o especializarlo según sea necesario, ha permitido crear de forma cada vez más rápida y confiable; para poner a disposición de un gran público programas de uso común, así como especializado que satisfagan las nuevas necesidades de los usuarios.

Software Libre en Ciencia y Educación Algunos puntos y reflexiones sobre porqué se considera que es interesante el Software libre en Ciencia y

Educación son:

- Accesible a todo el mundo aunque no sea rentable su desarrollo: El Software libre entre sus libertades permite que se pueda ejecutar por terceros, copiarlo, distribuirlo y estudiarlo/modificarlo. Eso hace que si en ciencia se usa Software libre el acceso a esos programas no suponga una barrera (se puede distribuir y ejecutar).

- Muchos de los desarrollos en el campo de la accesibilidad se realizan en universidades y son distribuidos como Software libre: Aunque no sea rentable muchas veces el desarrollo de herramientas de accesibilidad (no sea algo monetizable) en la universidad se consigue escapar a esa la lógica capitalista de solamente invertir en lo que pueda ofrecer beneficio económico.

- Transparencia: En ciencia es importante ver las costuras para comprobar si es verdad lo que se afirma, tener acceso al código fuente del Software empleado permite poder estudiarlo por si realiza algún cálculo mal.

- Propicia el espíritu crítico: Si no tienes acceso a las revistas o el acceso es privativo para los bolsillos de mucha gente no puedes comprobar la información. Se nos pide que seamos críticos con la información que se nos da del mundo científico pero no podemos entrenar el espíritu crítico sin acceso al conocimiento libre.

- Caramelos con droga en la puerta del colegio: Muchas empresas buscan introducir en los colegios, institutos y universidad su Software. Ofrecer un programa que permita trabajar y genere una dependencia quedando los datos muchas veces en las nubes (ordenadores de otras personas). Un ejemplo es Microsoft con Office 365. Dando cuentas gratuitas durante un tiempo para que se use su Software. Otro ejemplo podría ser Unity3D en vez de por ejemplo Godot.

- Especificaciones de protocolos abiertas VS cerradas: Gracias a que los protocolos TCP/IP, HTTP, POP, SNMP, DHCP, etc. son abiertos es posible construir herramientas por cualquier con conocimientos de programación. Con protocolos cerrados solamente quienes tuvieran acceso a las especificaciones podrían desarrollar y conocer cómo funcionan.

- Uso de estándares: Existiendo un estándar para documentos ofimáticos (procesador de textos, hoja de cálculo, presentaciones, etc.) algunas empresas como Microsoft se empeñan en ir con su propio formato y estándar en vez de sumarse a que sea más sencillo ir a una y que el usuario pueda optar por que herramientas usar para editar o trabajar con documentos ofimáticos.

- Software libre para la Ciencia ciudadana: Un ejemplo en el que es importante la colaboración ciudadana es el cambio climático y la defensa medioambiental del territorio. Desde imvec.tech usan herramientas de Software libre para medición y monitorización de contaminación.

Software Libre: Beneficios Más Allá de la Informática El uso de las tecnologías de código abierto supone cultivar el conocimiento y la puesta en valor de la libertad individual, lo personal y lo privado, todo ello sin menospreciar lo público y la construcción de una sociedad. El movimiento del Software libre, con Linux a la cabeza, ha capitaneado durante décadas planteamientos para un cambio en el modo de producción: el abaratamiento de costes empresariales para grandes y pequeños, el trabajo en línea, el desarrollo de Software y Hardware a pequeña escala, el replanteamiento del negocio informático, el sistema de normas éticas que rigen los grupos, la documentación abierta, etc.

Todo ello derivado de una simple idea: la libertad. Ha sido la clave que ha llevado a todo este movimiento hacia una autonomía y motivación que pocas veces se ve en otros sectores. El Open Source está lleno de alternativas con la libertad como pilar y consecuencia filosófica, de hecho muchos Forks (derivaciones) de proyectos aparecen cuando la disputa sobre la misma toma relevancia. Esta manera de hacer las cosas debería trasladarse directamente a la sociedad promoviendo esos valores para evitar caer en un mundo despótico que toma fuerza a pasos agigantados.

No estaría mal promover la comprensión de las licencias libres. Leer y entender una licencia GPL, MIT o BSD es infinitamente más sencillo y rápido que hacerlo con otras, siendo unas normas fáciles de cumplir porque encajan con un modelo ético y práctico comprensible por muchos.

Podríamos decir que GPL, BSD y MIT son las Constituciones que vertebran todo el movimiento del Software Libre, cosechando derechos de uso y logros como el ahorro o la legítima copia privada. Lo mismo podría ocurrir con las licencias Creative Commons para cierto contenido, un arma poderosa

en el sector divulgativo que está poco extendida por desconocimiento y el Status Quo de la propiedad intelectual.

La cooperación libre y voluntaria supuso un éxito hasta ahora pero está siendo amenazada por la dinámica actual de la Web, donde la centralización de las principales plataformas supone estar bajo el yugo de normas que rastrean con lupa y cambian sus términos con demasiada frecuencia. Ya ni digamos cuando eso se junta con el ansia de monetización: si quieres dinero más te vale no cabrear a los anunciantes o no tener un Strike por uso de contenido que podría ser reclamado.

Los claroscuros de este sistema hace que los creadores cada vez hagan menos de forma libre y altruista, y ello podría verse potenciado por las búsquedas con inteligencia artificial, lo que apunta a un empobrecimiento del contenido cultural fresco y renovador. Las polémicas con GitHub Copilot o ChatGPT sobre el entrenamiento de las IAs hace sobrevolar una vez más la cuestión del Copyright y el uso legítimo de los resultados brindados por éstas, lo que también condiciona la creación.

La libertad de expresión, de uso, de creación, de modificación ... esas cuestiones llevan irremediablemente a una libertad de pensamiento y acción, a una adaptación creativa que puede ser la motivación para romper moldes en todos los aspectos. El código abierto y sus licencias son, por tanto, un beneficio personal y social mucho más grande que el simple hecho de usar Linux o Software libre. El contenido despreocupado, que no prioriza el dinero y el posicionamiento/visualizaciones, se vuelve esencial para el inconformismo.

11.3 Seguridad del Software

Si bien, el Software Libre no es más seguro (en el sentido de invulnerable) que el propietario, la diferencia puede estribar en que el código fuente en el Software libre está disponible para todos y cualquiera puede aportar una solución y por lo general al poco tiempo de detectarse una vulnerabilidad (a veces en cuestión de horas) se puede disponer de una solución para la misma. Además, al tener acceso al código fuente se puede detectar si alguien introdujo código malicioso a una determinada aplicación.

Pero de todos es sabido, que los usuarios de Software de código abierto, como por ejemplo los que de manera habitual trabajan con equipos comandados por sistemas Linux, por regla general se sienten orgullosos de la seguridad que estos programas aportan con respecto a los sistemas cerrados propios de otras firmas, dígase Microsoft Windows o Mac de Apple.

¿Es Seguro el Software Libre? En primer lugar definiremos el concepto de "seguridad" como salvaguarda de las propiedades básicas de la información. Entre las características que debe cumplir para ser seguro, encontramos la integridad, es decir, que sólo los usuarios autorizados pueden crear y modificar los componentes del sistema, la confidencialidad, sólo estos usuarios pueden acceder a esos componentes, la disponibilidad, que todos los componentes estén a disposición de los usuarios siempre que lo deseen y el "no repudio", o lo que es lo mismo, la aceptación de un protocolo de comunicación entre el servidor y un cliente, por ejemplo, mediante certificados digitales.

Entre las diferencias de seguridad entre un Software Libre y el Software Propietario, podemos destacar:

- Seguridad en el Software Propietario: En el caso de tener "agujeros de seguridad", puede que no nos demos cuenta y que no podamos repararlos. Existe una dependencia del fabricante, retrasándose así cualquier reparación y la falsa creencia de que es más seguro por ser oscuro (la seguridad por oscuridad determina los fallos de seguridad no parcheados en cada producto).

- Seguridad en el Software Libre: Por su carácter público y su crecimiento progresivo, se van añadiendo funciones y se nos permite detectar más fácilmente los agujeros de seguridad para poder corregirlos. Los problemas tardan mucho menos en ser resueltos por el apoyo que tiene de los Hackers y una gran comunidad de desarrolladores y al ser un Software de código libre, cualquier empresa puede aportar soporte técnico.

Sin embargo esta es una pregunta sobre la que los expertos al día de hoy, tras muchos años de discusiones, siguen sin ponerse de acuerdo. ¿Es más seguro el Software de código abierto que los programas cerrados, o viceversa? Lo cierto es que, en términos generales, ambos bandos tienen sus razones con las que defender sus argumentos. Por un lado, los usuarios de las aplicaciones y sistemas de código abierto, defienden que, al estar el código fuente disponible a los ojos de todo el mundo, es mucho más fácil localizar posibles agujeros de seguridad y vulnerabilidades que pongan en peligro los datos de los usuarios.

Por otro lado, aquellos que consideran que los sistemas cerrados son más seguros en este sentido, afirman que al tener acceso tan solo los expertos al código fuente de sus aplicaciones, es más complicado que se produzcan

filtraciones o inserciones de Software malicioso en este tipo de sistemas. Hay que tener en cuenta que, por ejemplo, Google premia a las personas que descubren fallos de seguridad en su Software como Chrome, aunque no es el único gigante de la tecnología en utilizar estas tácticas.

De hecho muchas empresas están gastando miles de millones de dólares y/o euros en hacer que sus propuestas sean lo más seguras posible, argumentando que la seguridad de sus proyectos es una de sus prioridades, todo con el fin de intentar frenar que los atacantes vulneren sus sistemas. Por otro lado, otros aseguran que cuando el código fuente es público, más ojos están disponibles para detectar posibles vulnerabilidades o errores en dicho código, por lo que siempre será más rápido y sencillo poner soluciones con el fin de ganar en seguridad.

Sea como sea, en cualquiera de los dos casos, lo que ha quedado más que demostrado es que la seguridad no está garantizada en ningún momento, ya sean propuestas de código abierto, o no. Pero también es cierto que lo que se procura es que los riesgos de ser atacados se reduzcan en medida de lo posible. Los sistemas Linux son considerados desde hace mucho tiempo como un sistema operativo seguro, en buena parte debido a las ventajas que ofrece su diseño. Dado que su código está abierto, son muchas las personas que incorporan mejoras de las que el resto de usuarios de Linux se benefician, a diferencia de las propuestas de Windows o MacOS, donde estas correcciones generalmente se limitan a las que detectan Microsoft y Apple.

No obstante, en nuestra defensa del Software libre, diremos que su código abierto permite que los errores sean encontrados y solucionados con mayor rapidez, por lo que determinamos que es el Software más recomendable.

En general, puede afirmarse que el Software libre es más seguro, ya que debido a su carácter abierto y distribuido, un gran número de programadores y personas expertas pueden estar atentas al código fuente -especialmente en los grandes proyectos-, lo cual permite hacer auditorías con objeto de detectar errores y puertas traseras (Backdoor, en inglés) que pongan en riesgo nuestros datos.

Así, los grandes programas y proyectos de Software libre, con una extensa comunidad de desarrollo y usuarios que lo respalden, presentan niveles muy altos de seguridad, un alto grado de protección y una rápida respuesta a posibles vulnerabilidades.

11.4 Tipos de Licencias

Tanto la Open Source Initiative como la Free Software Foundation mantienen en sus páginas Web (véase [12], [13], y [11]) listados oficiales de las licencias de Software libre que aprueban.

Una licencia es aquella autorización formal con carácter contractual que un autor de un Software da a un interesado para ejercer "actos de explotación legales". Pueden existir tantas licencias como acuerdos concretos se den entre el autor y el licenciatario. Desde el punto de vista del Software libre, existen distintas variantes del concepto o grupos de licencias:

Licencias GPL Una de las más utilizadas es la Licencia Pública General de GNU (GNU GPL). El autor conserva los derechos de autoría (Copyright), y permite la redistribución y modificación bajo términos diseñados para asegurarse de que todas las versiones modificadas del Software permanecen bajo los términos más restrictivos de la propia GNU GPL. Esto hace que sea imposible crear un producto con partes no licenciadas GPL, el conjunto tiene que ser GPL.

En la práctica, esto hace que las licencias de Software libre se dividan en dos grandes grupos, aquellas que pueden ser mezcladas con código licenciado bajo GNU GPL (y que inevitablemente desaparecerán en el proceso, al ser el código resultante licenciado bajo GNU GPL) y las que no lo permiten al incluir mayores u otros requisitos que no contemplan ni admiten la GNU GPL y que por lo tanto no pueden ser enlazadas ni mezcladas con código gobernado por la licencia GNU GPL.

GPL Versión 1 la versión 1 de GNU GPL, fue presentada el 25 de febrero de 1989, impidió lo que eran las dos principales formas con las que los distribuidores de Software restringían las libertades definidas por el Software libre. El primer problema fue que los distribuidores publicaban únicamente los archivos binarios, funcionales y ejecutables, pero no entendibles o modificables por humanos. Para prevenir esto, la GPLv1 estableció que cualquier proveedor de Software libre además de distribuir el archivo binario debía liberar a su vez código fuente entendible y que pudiera ser modificado por el ser humano bajo la misma licencia (secciones 3a y 3b de la licencia).

El segundo problema era que los distribuidores podían añadir restricciones adicionales, añadiendo restricciones a la licencia o mediante la combinación del Software con otro que tuviera otras restricciones en su distribución. Si

esto se hacía, entonces la unión de los dos conjuntos de restricciones sería aplicada al trabajo combinado, entonces podrían añadirse restricciones inaceptables. Para prevenir esto, GPLv1 obligaba a que las versiones modificadas en su conjunto, tuvieran que ser distribuidas bajo los términos GPLv1 (secciones 2b y 4 de la licencia). Por lo tanto, el Software distribuido bajo GPLv1 puede ser combinado con Software bajo términos más permisivos y no con Software con licencias más restrictivas, lo que entraría en conflicto con el requisito de que todo Software tiene que ser distribuido bajo los términos de la GPLv1.

GPL Versión 2 según Richard Stallman, el mayor cambio en GPLv2 fue la cláusula "Liberty or Death" («libertad o muerte»). Esta sección dice que si alguien impone restricciones que le prohíben distribuir código GPL de tal forma que influya en las libertades de los usuarios (por ejemplo, si una ley impone que esa persona únicamente pueda distribuir el Software en binario), esa persona no puede distribuir Software GPL. La esperanza es que esto hará que sea menos tentador para las empresas el recurrir a las amenazas de patentes para exigir una remuneración de los desarrolladores de Software libre.

En 1991 se hizo evidente que una licencia menos restrictiva sería estratégicamente útil para la biblioteca C y para las bibliotecas de Software que esencialmente hacían el trabajo que llevaban a cabo otras bibliotecas comerciales ya existentes. Cuando la versión 2 de GPL fue liberada en junio de 1991, una segunda licencia Library General Public License fue introducida al mismo tiempo y numerada con la versión 2 para denotar que ambas son complementarias. Los números de versiones divergieron en 1999 cuando la versión 2.1 de LGPL fue liberada, esta fue renombrada como GNU Lesser General Public License para reflejar su lugar en esta filosofía.

GPL Versión 3 A finales de 2005, la Free Software Foundation (FSF) anunció estar trabajando en la versión 3 de la GPL (GPLv3). El 16 de enero de 2006, el primer borrador de GPLv3 fue publicado y se inició la consulta pública. La consulta pública se planeó originalmente para durar de nueve a quince meses, pero finalmente se extendió a dieciocho meses, durante los cuales se publicaron cuatro borradores. La GPLv3 oficial fue liberada por la FSF el 29 de junio de 2007.

Según Stallman los cambios más importantes se produjeron en el campo

de las patentes de Software, la compatibilidad de licencias de Software libre, la definición de código fuente y restricciones a las modificaciones de Hardware. Otros cambios están relacionados con la internacionalización, cómo son manejadas las violaciones de licencias y cómo los permisos adicionales pueden ser concedidos por el titular de los derechos de autor. También añade disposiciones para quitar al DRM su valor legal, por lo que es posible romper el DRM (Digital Rights Management) en el Software de GPL sin romper leyes como la DMCA (Digital Millennium Copyright Act).

GPLv2 vs GPL v3 GPLv3 contiene la intención básica de GPLv2 y es una licencia de código abierto con un Copyleft estricto. Sin embargo, el idioma del texto de la licencia fue fuertemente modificado y es mucho más completo en respuesta a los cambios técnicos, legales y al intercambio internacional de licencias.

La nueva versión de la licencia contiene una serie de cláusulas que abordan preguntas que no fueron o fueron cubiertas de manera insuficiente en la versión 2 de la GPL. Las nuevas regulaciones más importantes son las siguientes:

- GPLv3 contiene normas de compatibilidad que hacen que sea más fácil combinar el código GPL con el código que se publicó bajo diferentes licencias. Esto se refiere en particular al código bajo la licencia de Apache v. 2.0.

- Se insertaron normas sobre gestión de derechos digitales para evitar que el Software GPL se modifique a voluntad, ya que los usuarios recurrieron a las disposiciones legales para protegerse mediante medidas técnicas de protección (como la DMCA o la directiva sobre derechos de autor).

- La licencia GPLv3 contiene una licencia de patente explícita, según la cual las personas que licencian un programa bajo licencia GPL otorgan derechos de autor y patentes, en la medida en que esto sea necesario para utilizar el código que ellos otorgan. Por lo tanto, no se concede una licencia de patente completa. Además, la nueva cláusula de patente intenta proteger al usuario de las consecuencias de los acuerdos entre los titulares de patentes y los licenciatarios de la licencia pública general que solo benefician a algunos de los licenciatarios (correspondientes al

acuerdo Microsoft / Novell). Los licenciatarios deben garantizar que todos los usuarios disfrutan de tales ventajas (licencia de patente o liberación de reclamos) o que nadie puede beneficiarse de ellos.

- A diferencia de la GPLv2, la GPLv3 establece claramente que no es necesario divulgar el código fuente en un uso ASP (Application Service Provider) de los programas GPL, siempre que no se envíe una copia del Software al cliente. Si el efecto Copyleft debe extenderse al uso de ASP, debe aplicarse la Licencia pública general de Affero, versión 3 (AGPL) que solo difiere de la GPLv3 en esta consideración.

Licencias Estilo BSD Llamadas así porque se utilizan en gran cantidad de Software distribuido junto a los sistemas operativos BSD. El autor, bajo tales licencias, mantiene la protección de Copyright únicamente para la renuncia de garantía y para requerir la adecuada atribución de la autoría en trabajos derivados, pero permite la libre redistribución y modificación, incluso si dichos trabajos tienen propietario. Son muy permisivas, tanto que son fácilmente absorbidas al ser mezcladas con la licencia GNU GPL con quienes son compatibles. Puede argumentarse que esta licencia asegura "verdadero" Software libre, en el sentido que el usuario tiene libertad ilimitada con respecto al Software y que puede decidir incluso redistribuirlo como no libre.

Licencia Copyleft Hay que hacer constar que el titular de los derechos de autor (Copyright) de un Software bajo licencia Copyleft puede también realizar una versión modificada bajo su Copyright original y venderla bajo cualquier licencia que desee, además de distribuir la versión original como Software libre. Esta técnica ha sido usada como un modelo de negocio por una serie de empresas que realizan Software libre (por ejemplo MySQL); esta práctica no restringe ninguno de los derechos otorgados a los usuarios de la versión Copyleft.

Licencia estilo MIT Las licencias MIT son de las más permisivas, casi se consideran Software de dominio público. Lo único que requieren es incluir la licencia MIT para indicar que el Software incluye código con licencia MIT.

Licencia Apache License La licencia Apache trata de preservar los derechos de autor, incluir la licencia en el Software distribuido y una lista de

los cambios realizados. En modificaciones extensivas del Software original permite licenciar el Software bajo otra licencia sin incluir esas modificaciones en el código fuente.

Licencia Mozilla Public License MPL Esta licencia requiere que los archivos al ser distribuidos conserven la misma licencia original pero pueden ser usados junto con archivos con otra licencia, al contrario de la licencia GPL que requiere que todo el código usado junto con código GPL sea licenciado como código GPL. También en caso de hacer modificaciones extensivas permite distribuirlas bajo diferentes términos y sin incluir el código fuente en las modificaciones.

Licencia Código de Dominio Público Es un código que no está sujeto a derechos de autor que puede utilizarse sin restricciones.

Licencia Creative Commons Las licencias de Creative Commons son más utilizadas para cualquier creación digital que para el Software, entendiendo como creación digital desde fotos, artículos en blogs, música, vídeos, este trabajo, etc. Hay varios tipos de licencias de Creative Commons diferenciando entre permitir modificaciones a la obra original, solicitando crédito de la creación o permitiendo un uso comercial de la obra.

Licencias de Código Abierto Las licencias de código abierto son un intermedio entre las licencias privativas y las licencias de Software libre. Las licencias de código abierto permiten el acceso al código fuente pero no todas se consideran licencias de Software libre al no otorgar otros derechos que se requieren para considerar un Software como Software libre como el derecho al uso o con cualquier propósito, modificación y distribución.

Dado el éxito del Software libre como modelo de desarrollo de Software algunas empresas cuyo Software era privativo pueden decidir hacerlo de código abierto con la intención de suplir algunas carencias de Software privativo pero sin perder ciertos derechos que son la fuente de sus ingresos como la venta de licencias.

Las expresiones «Software libre» y «código abierto» se refieren casi al mismo conjunto de programas. No obstante, dicen cosas muy diferentes acerca de dichos programas, basándose en valores diferentes. El movimiento del Software libre defiende la libertad de los usuarios de ordenadores, en un

movimiento en pro de la libertad y la justicia. Por contra, la idea del código abierto valora principalmente las ventajas prácticas y no defiende principios. Esta es la razón por la que gran parte de la comunidad de Software libre está en desacuerdo con el movimiento del código abierto y nosotros no empleamos esta expresión en este texto.

Licencia Microsoft Public License La Microsoft Public License es una licencia de código abierto que permite la distribución del Software bajo la misma licencia y la modificación para un uso privado. Tiene restricciones en cuanto a las marcas registradas.

En caso de distribuir el Software de forma compilada o en forma de objeto binario no se exige proporcionar los derechos de acceso al código fuente del Software compilado o en forma de objeto binario. En este caso esta licencia no otorga más derechos de los que se reciben, pero si permite otorgar menos derechos al distribuir el Software (compilado o en forma de objeto binario).

Modelo de Desarrollo de Software Bazar y Catedral El tipo de licencia no determina qué Software es mejor o peor, si el privativo o el Software libre, la diferencia entre las licencias está en sus características éticas y legales. Aunque el modelo de desarrollo con una licencia de código abierto a la larga suele tener un mejor desarrollo y éxito que el Software privativo, más aún con un medio como internet que permite colaborar a cualquier persona independiente de donde esté ubicada en el mundo.

Comparación con el Software de Código Abierto Aunque en la práctica el Software de código abierto y el Software libre comparten muchas de sus licencias, la Free Software Foundation opina que el movimiento del Software de código abierto es filosóficamente diferente del movimiento del Software libre. Los defensores del término «código abierto (Open Source)», afirman que éste evita la ambigüedad del término en ese idioma que es «Free» en «Free Software».

Mucha gente reconoce el beneficio cualitativo del proceso de desarrollo de Software cuando los desarrolladores pueden usar, modificar y redistribuir el código fuente de un programa. El movimiento del Software libre hace especial énfasis en los aspectos morales o éticos del Software, viendo la excelencia técnica como un producto secundario de su estándar ético. El movimiento de código abierto ve la excelencia técnica como el objetivo prioritario, siendo

el compartir el código fuente un medio para dicho fin. Por dicho motivo, la FSF se distancia tanto del movimiento de código abierto como del término «código abierto (Open Source)».

Puesto que la «iniciativa de Software libre Open Source Initiative (OSI)» sólo aprueba las licencias que se ajustan a la «definición de código abierto (Open Source Definition)», la mayoría de la gente lo interpreta como un esquema de distribución, e intercambia libremente "código abierto" con "Software libre". Aún cuando existen importantes diferencias filosóficas entre ambos términos, especialmente en términos de las motivaciones para el desarrollo y el uso de tal Software, raramente suelen tener impacto en el proceso de colaboración.

Aunque el término "código abierto" elimina la ambigüedad de libertad frente a precio (en el caso del inglés), introduce una nueva: entre los programas que se ajustan a la definición de código abierto, que dan a los usuarios la libertad de mejorarlos y los programas que simplemente tienen el código fuente disponible, posiblemente con fuertes restricciones sobre el uso de dicho código fuente. Mucha gente cree que cualquier Software que tenga el código fuente disponible es de código abierto, puesto que lo pueden manipular, sin embargo, mucho de este Software no da a sus usuarios la libertad de distribuir sus modificaciones, restringe el uso comercial, o en general restringe los derechos de los usuarios.

11.4.1 Licencias Creative Commons

Las Licencias[108] Creative Commons (CC) de forma general no tienen una definición oficial, sin embargo, entre las muchas definiciones aceptadas están la de la UNESCO, la cual expresa la siguiente descripción:

Las Licencias Creative Commons (CC) son modelos de contratos que sirven para otorgar públicamente el derecho de utilizar una publicación protegida por los derechos de autor. Entre menos restricciones implique una licencia, mayores serán las posibilidades de utilizar y distribuir un contenido. Las Licencias CC permiten a cualquier usuario descargar, copiar, distribuir, traducir, reutilizar, adaptar y desarrollar su contenido sin costo alguno.

Sin embargo, en la Web oficial de la Organización Creative Commons se nos dice sobre las mismas lo siguiente:

[108] Las licencias de Creative Commons son más utilizadas para cualquier creación digital que para el Software, entendiendo como creación digital desde fotos, artículos en blogs, música, vídeos, este trabajo, etc.

Las Licencias Creative Commons (CC) brindan a todos, desde creadores individuales hasta grandes instituciones, una forma estandarizada de otorgar permiso al público para usar su trabajo creativo bajo la ley de derechos de autor. Desde la perspectiva del reutilizador, la presencia de una licencia Creative Commons sobre una obra protegida por derechos de autor responde a la pregunta: ¿Qué puedo hacer con esta obra?.

Las «Licencias Creative Commons» que hoy en día pertenecen a la organización mundial Creative Commons[109], y buscan regularizar y mantener, de forma equilibrada y satisfactoria, todo lo relacionado con el derecho de utilizar una publicación protegida por los derechos de autor a nivel mundial, han logrado un buen trabajo, sin duda alguna. Y seguramente en el tiempo, se irán adaptando a las nuevas realidades sociales y tecnológicas para poder seguir manteniendo de forma armónica las posibilidades de utilizar y distribuir cualquier contenido libre y abierto sobre la Internet, y más allá.

¿Cuáles son y cómo funcionan o para qué se usan? Las 7 distintas Licencias Creative Commons son las siguientes:

CC BY Esta licencia permite a los reutilizadores distribuir, remezclar, adaptar y desarrollar el material en cualquier medio o formato, siempre que se otorgue la atribución al creador. La licencia permite el uso comercial.

CC BY-SA Esta licencia permite a los reutilizadores distribuir, remezclar, adaptar y desarrollar el material en cualquier medio o formato, siempre que se otorgue la atribución al creador. La licencia permite el uso comercial. Si remezcla, adapta o construye sobre el material, debe licenciar el material modificado bajo términos idénticos.

CC BY-NC Esta licencia permite a los reutilizadores distribuir, remezclar, adaptar y desarrollar el material en cualquier medio o formato, únicamente con fines no comerciales y siempre que se otorgue la atribución al creador.

[109] Una organización mundial sin ánimo de lucro que permite compartir y reutilizar la creatividad y el conocimiento mediante el suministro de herramientas legales gratuitas. Y cuyas herramientas legales (licencias) ayudan a quienes quieren fomentar la reutilización de sus obras ofreciéndolas para su uso bajo términos generosos y estandarizados; a quienes quieren hacer usos creativos de las obras; y a quienes quieren beneficiarse de esta simbiosis.

CC BY-NC-SA Esta licencia permite a los reutilizadores distribuir, remezclar, adaptar y desarrollar el material en cualquier medio o formato, únicamente con fines no comerciales y siempre que se otorgue la atribución al creador. Si remezcla, adapta o construye sobre el material, debe licenciar el material modificado bajo términos idénticos.

CC BY-ND Esta licencia permite a los reutilizadores copiar y distribuir el material en cualquier medio o formato únicamente en forma no adaptada, y siempre y cuando se otorgue la atribución al creador. La licencia permite el uso comercial.

CC BY-NC-ND Esta licencia permite a los reutilizadores copiar y distribuir el material en cualquier medio o formato únicamente en forma no adaptada, únicamente con fines no comerciales y siempre que se otorgue la atribución al creador.

CC0 (CC Cero) Esta licencia es una herramienta de dedicación pública que permite a los creadores renunciar a sus derechos de autor y poner sus obras en el dominio público mundial. CC0 permite a los reutilizadores distribuir, remezclar, adaptar y desarrollar el material en cualquier medio o formato, sin condiciones.

11.4.2 Nuevas Licencias para Responder a Nuevas Necesidades

El mundo de la tecnología avanza mucho más rápido que las leyes y estas tienen que esforzarse para alcanzarlo. En el caso del Software libre y de código abierto, tanto la Free Software Foundation como la Open Source Initiative (los organismos encargados de regular las diferentes licencias) enfrentan periódicamente el problema de cómo mantener sus principios y al mismo tiempo evitar que alguien se aproveche indebidamente.

En el último tiempo, la Open Source Initiative le dio el sello de aprobación a otras nuevas licencias para propósitos específicos.

Nuevas Licencias de Código Abierto

- Cryptographic Autonomy License version 1.0 (CAL-1.0)

Fue creada en el 2019 por el equipo del proyecto de código abierto Holochain, esta licencia fue desarrollada para ser utilizada con aplicaciones criptográficas distribuidas. El inconveniente con las licencias tradicionales es que no obligaba a compartir los datos. Esto podría perjudicar el funcionamiento de toda la red. Por eso la CAL también incluye la obligación de proporcionar a terceros los permisos y materiales necesarios para utilizar y modificar el Software de forma independiente sin que ese tercero tenga una pérdida de datos o capacidad.

- Open Hardware Licence (OHL)

De la mano de la Organización Europea para la Investigación Nuclear (CERN) llegó esta licencia con tres variantes enfocadas en la posibilidad de compartir libremente tanto Hardware como Software.

Hay que hacer una aclaración. La OSI fue creada en principio pensando en el Software por lo que no tiene mecanismos para la aprobación de licencias de Hardware. Pero, como la propuesta del CERN se refiere a ambos rubros, esto posibilitó la aprobación:

- CERN-OHL-S es una licencia fuertemente recíproca: El que utilice un diseño bajo esta licencia deberá poner a disposición las fuentes de sus modificaciones y agregados bajo la misma licencia.
- CERN-OHL-W es una licencia débilmente recíproca: Sólo obliga a distribuir las fuentes de la parte del diseño que fue puesta originalmente bajo ella. No así los agregados y modificaciones.
- CERN-OHL-P es una licencia permisiva: Permite a la gente tomar un proyecto, relicenciarlo y utilizarlo sin ninguna obligación de distribuir las fuentes.

Hay que decir que la gente del CERN parece haber encontrado la solución a un problema que viene afectando a algunos proyectos de código abierto. Una gran empresa utiliza ese proyecto para comercializar servicios y no solo hace ningún aporte al proyecto original (ya sea con código o dando apoyo financiero) si no que también compite en el mismo mercado.

Post Open Zero-Cost en el año 2024 se desarrolla la licencia «Post Open Zero-Cost» con la cual busca abordar los desafíos surgidos en la interacción entre desarrolladores de código abierto y empresas comerciales, especialmente en lo que respecta a la compensación justa por el uso comercial del código.

La característica distintiva de la licencia «Post-Open» en comparación con las licencias abiertas existentes, como la GPL, es la introducción de un componente contractual que puede ser rescindido en caso de violación de los términos. Esta licencia ofrece dos tipos de acuerdos contractuales: gratuitos y de pago. El acuerdo de pago permite negociar derechos adicionales para la distribución comercial de productos o modificaciones sin requerir su divulgación pública.

Las situaciones que podrían llevar a la terminación del acuerdo contractual incluyen: violación de los términos de la licencia; reclamaciones por infracción de patentes; imposición de condiciones adicionales (como sanciones en contratos con clientes por divulgación de información sensible); cambios sujetos a leyes de control de exportaciones; ocultamiento de información sobre vulnerabilidades; y uso del código para entrenamiento de modelos de aprendizaje automático bajo términos no permitidos. Las relaciones contractuales no se rescinden de inmediato, sino que se notifica la infracción y se otorgan 60 días para corregirla antes de la rescisión efectiva del acuerdo.

Uno de los problemas que la nueva licencia busca abordar está relacionado con las limitaciones de la GPL, la cual se centra en otorgar derechos sin la capacidad de revocarlos, lo que permite a las empresas encontrar formas de eludir sus requisitos, especialmente en lo que respecta al acceso al código fuente. Estas lagunas son utilizadas para restringir la disponibilidad del código subyacente en productos comerciales mediante la imposición de términos contractuales adicionales con los usuarios finales.

Un claro ejemplo es el de RHEL, la cual los clientes firman un acuerdo con Red Hat que limita la redistribución del código fuente al imponer condiciones sobre la coincidencia de las copias instaladas y compradas de RHEL. Esto coloca a los usuarios en la disyuntiva entre su libertad para disponer del software y mantener su estatus de cliente de Red Hat. Aunque la GPL permite la distribución de parches que solucionan vulnerabilidades en el código de RHEL, esto podría interpretarse como una violación del acuerdo con Red Hat y podría resultar en la terminación de los servicios por parte de la empresa.

11.5 Implicaciones Económico-Políticas del Software Libre

Una vez que un producto de Software libre ha empezado a circular, rápidamente está disponible a un costo muy bajo. Al mismo tiempo, su utilidad no decrece. El Software, en general, podría ser considerado un bien de uso inagotable, tomando en cuenta que su costo marginal es pequeñísimo y que no es un bien sujeto a rivalidad -la posesión del bien por un agente económico no impide que otro lo posea-.

11.5.1 Software Libre y la Piratería

Puesto que el Software libre permite el libre uso, modificación y redistribución, a menudo encuentra un hogar entre usuarios para los cuales el coste del Software no libre es a veces prohibitivo, o como alternativa a la piratería. También es sencillo modificarlo localmente, lo que permite que sean posibles los esfuerzos de traducción a idiomas que no son necesariamente rentables comercialmente, además:

- Porque así no se condiciona a los usuarios a usar siempre lo mismo.
- Porque así no se fomenta la piratería en los usuarios al no pagar licencias.
- Porque así no se obliga a usar una solución concreta y se ofrece libertad de elección a los usuarios.
- Porque es mucho más seguro ya que el Software libre es público y se puede ver qué hace exactamente sin recelos.

La mayoría del Software libre se produce por equipos internacionales que cooperan a través de la libre asociación. Los equipos están típicamente compuestos por individuos con una amplia variedad de motivaciones y pueden provenir tanto del sector privado, del sector voluntario o del sector público. En los últimos años se ha visto un incremento notable de grandes corporativos (como IBM, Microsoft, Intel, Google, Samsung, Red Hat, etc.) que han dedicado una creciente cantidad de recursos humanos y computacionales para desarrollar Software libre, ya que esto apoya a sus propios negocios.

11.5.2 ¿Cuánto Cuesta el Software Libre?

En esta sección intentaremos dar una idea de cuál es el costo del desarrollo del Software Libre, por supuesto que no se tratará más que de una conjetura aproximada basada en las cifras proporcionadas por desarrolladores de Software comercial (al año 2020).

Gratis no Significa Gratuito Supongamos que todos los recursos humanos participantes en el desarrollo de un proyecto de Software libre lo hagan de forma voluntaria. De todas formas tenemos lo que los contables llaman «Costo de oportunidad» esto es, los ingresos que podrían haber generado esas personas si hubieran dedicado el tiempo y los conocimientos invertidos en el proyecto a uno en el que les pagaran. Así, el calcular el costo promedio por hora que cobra un programador, por la cantidad de horas invertidas al proyecto, nos da un razonable costo mínimo. Lo mismo puede hacerse con los voluntarios dedicados a la difusión en las redes. El costo de una campaña de marketing digital puede estimarse fácilmente.

Muchos proyectos de código abierto como una distribución Linux, son construidos a partir de la integración de otros proyectos, por los que sus costos de desarrollo también deberían sumarse.

Por otra parte, necesitamos recursos físicos. Aún cuando los voluntarios trabajen desde su casa, siguen teniendo que comprar y mantener sus equipos, además de pagar la electricidad que los hace funcionar.

Bases para el Cálculo Hay muchos factores que determinan el costo de desarrollar una pieza de Software. En un extremo tenemos una aplicación simple que requiere muy poca interacción del usuario o procesamiento del lado del servidor. Tal es el caso de un cliente de escritorio para redes sociales. Por el otro sistemas operativos que deben operar en múltiples plataformas realizando múltiples tareas (por ejemplo Debían que aspira a ser el sistema operativo universal). Sin embargo, el costo de una aplicación simple puede elevarse debido a que tiene múltiples pantallas diferentes. Por ejemplo un juego desarrollado con HTML5 y Javascript.

Los dos aspectos claves son la cantidad de horas de trabajo necesarias y las tecnologías involucradas. Para una aplicación de escritorio como un procesador de textos con las prestaciones habituales, optimizado para un determinado escritorio Linux, se estima que se tendría que contar con al menos el equivalente a 42,000 euros en trabajo voluntario. Un gestor de contenidos

para comercio electrónico con seguimiento de pedidos e integración con las principales plataformas de pago implicaría desembolsar unos 210,000 euros o su equivalente en trabajo voluntario.

Tomando en cuenta que este cálculo incluye lo que costó el desarrollo de las bibliotecas y otros proyectos libres y de código abierto incluidos, pero no los gastos que efectivamente deben desembolsarse en efectivo como la compra de equipos, Software de seguridad y desarrollo y el pago de electricidad e internet.

Por otro lado, el proceso de medición de costes del Software es un factor realmente importante en el análisis de un proyecto. Hay distintos métodos de estimación de costes de desarrollo de Software (también conocido como métrica del Software). La gran mayoría de estos métodos se basan en la medición del número de Líneas de Código que contiene el desarrollo (se excluyen comentarios y líneas en blanco de los fuentes).

Desarrollo de Fedora 9 La Linux Foundation ha calculado que costaría desarrollar el código de la distribución Fedora 9 que fue puesta a disposición del público el 13 de mayo de 2008, en el informe citado "Estimating the Total Development Cost of a Linux Distribution" se calcula que Fedora 9 tiene un valor de 10.8 mil millones de dólares y que el coste únicamente del Kernel (2.6.25 con 8,396,250 líneas de código) tendría un valor de 1.4 mil millones de dólares.

Esta distribución tiene unas 205 millones de líneas de código, el proyecto debería ser desarrollado por 1000 - 5000 desarrolladores (el trabajo invertido por una única persona desarrollándolo se alargaría durante unos 60.000 años) y esa estimación no va muy desencaminada ya que en los 2 últimos años del desarrollo de esa versión contribuyeron unos 3,200 desarrolladores aunque el número de trabajadores en la historia de la distribución es mucho mayor.

¿Qué pasa con GNU/Linux? en el año 2015 (las estadísticas más actuales que conseguimos) la Linux Foundation analizó el costo de desarrollo del núcleo. Combinando el aporte de los recursos humanos (voluntarios y de pago) y los desembolsos necesarios, la cuenta sumó 476,767,860,000.13 euros.

Todos sabemos que el hecho de tener desarrolladores asalariados no garantiza necesariamente Software de calidad. Pero, tener desarrolladores que pueden dedicar toda su atención a un proyecto en lugar de hacerlo en sus horas libres si lo hace. Lamentablemente, por el momento el único modo de

lograr eso es obtener el apoyo de corporaciones (Intel, Google, IBM, AMD, Sun Microsystems, Dell, Lenovo, Asus, HP, SGI, Oracle, RedHat, etc.) que solo lo hacen con los proyectos que son de su interés como el Kernel de Linux, hay que notar que para el Kernel de Linux un porcentaje importante (más del 10 %) lo hacen programadores independientes.

Costes Recordemos que la segunda de las cuatro libertades de un programa para ser Software libre es:

- Libre redistribución

y esta puede ser a través de un pago o sin costo. Es por ello que existen distintas empresas, organizaciones y usuarios que pueden apoyar a los usuarios finales en el desarrollo y soporte de algún programa de Software libre o una distribución personalizada de Linux por un costo determinado.

Mucha gente, en especial ejecutivos de empresas, se acercan a Linux bajo la promesa de que es una solución de bajo costo -muchos piensan que incluso es gratis-. Pero la realidad es que detrás de Linux y los programas de Software libre (y aquí la traducción correcta de la palabra inglesa, Free es libre, no gratis) pueden llevar una serie de costos ocultos que deben ser considerados al momento de decidir si se implementa una solución propietaria o una libre.

Los costos ocultos aparecen cuando se intenta instalar y capacitar en el uso de algún Software y se necesita la ayuda de un informático, al que se tiene que pagar, o alguna empresa quiere personalizar la interfaz de un programa y necesita la ayuda de un programador, que también tienen un coste, por lo que finalmente el comentario suele ser "el Software libre no es barato".

El primer punto a considerar al evaluar ambas alternativas es el costo de la licencia. Los productos de Software libre no suelen tener un costo de licencia asociado, que sí existe en los programas propietarios. De hecho es allí en donde los fabricantes de Software recargan sus costos de investigación y desarrollo, de producción e incluso sus ganancias. En este primer punto el ganador claro es el Software libre y es lo que los adeptos de este esquema publicitan: "su compañía puede ahorrar miles de dólares al año usando Software libre".

El segundo punto a considerar es el costo de instalación, configuración y capacitación. Dependiendo de su complejidad, algunos productos comerciales no contemplan costos extra por este concepto y otros -como Windows, por ejemplo- son tan populares que se puede encontrar numerosas opciones

de instalación -a través de empresas o profesionales- donde escoger en el mercado. A veces en el Software libre la configuración puede implicar recompilar el producto con algunas opciones particulares, algo que sólo pueden realizar técnicos con un nivel adecuado de conocimientos y que puede que no sean tan fáciles de encontrar. Aquí por lo general la ventaja va hacia el Software comercial.

Una vez instalado el Software, toca realizar actualizaciones de mantenimiento. Si bien es cierto lo que algunos de los fanáticos del Software libre dicen, que nadie lo obliga a mejorar el Software con que cuenta, la realidad -especialmente en lo que a seguridad se refiere- obliga a las empresas a mantener su Software actualizado. Aún así, los costos de actualizar Software libre suelen ser significativamente más bajos que los de productos comerciales y suelen ser menos exigentes con el Hardware necesario para ejecutarlos. La mayoría de las veces la ventaja es para el Software libre, pero hay que evaluar ya que varía dependiendo de cada caso.

Por último hay algunas casas que desarrollan productos de Software libre -dan el código y permiten que cualquiera lo modifique o reutilice- pero fijan contratos con cargos mensuales o anuales para mantenimiento del mismo, algo que se parece mucho a un cobro por licencia, por lo que hay que estar seguro de conocer todas las condiciones cuando una empresa nos ofrece una solución propia y la califica como Software libre.

Además de estas consideraciones hay una que debe sumarse eventualmente a esta evaluación: el costo de migrar a otra solución. En Software libre suelen usarse estándares abiertos para almacenar los datos, lo que facilita las migraciones. En cambio muchas soluciones propietarias suelen tener formatos propietarios que pueden dejar "amarrados" los datos de la empresa a una aplicación específica.

Sólo después de evaluar estos aspectos del Software, que pueden tener implicaciones importantes en el presupuesto, es que un CIO (Chief Information Officer) puede decir si una solución de Software libre le conviene más a una empresa o no, algo que va más allá de que la aplicación sea gratis o no.

11.5.3 La Nube y el Código Abierto

Desde hace años se han creado nuevos desafíos para el código abierto que plantea la nube, un término que para el usuario promedio puede significar cosas diferentes, pero que para la empresa se resume en servicios. Y es que los beneficios económicos que genera el mero Software de código abierto no

son comparables a los que se obtienen cuando se ofrece ese mismo Software a través de servicios, más allá -pero incluyendo- del soporte.

Este hecho diferencial lleva tiempo provocando fricciones entre desarrolladores y proveedores y hay quien adelantó incluso el fin del modelo de desarrollo del código abierto tal y como lo conocemos. ¿Quién tiene la razón?, ¿es para tanto la situación?.

En sus exposiciones, representantes de compañías y proyectos de código abierto muy populares en el ámbito empresarial, explican el supuesto perjuicio que les ocasiona el uso que los grandes proveedores de servicios en la nube hacen del Software que ellos desarrollan y cómo algunos han considerado y aplicado un enfoque más cerrado para sus productos con el fin de evitar lo que denominan como expolio. Hay declaraciones que merecen ser rescatadas para dotar de contexto a la discusión:

- El papel que juega el código abierto en la creación de oportunidades comerciales ha cambiado, durante muchos años les permitimos que las empresas de servicios tomaran lo que se ha desarrollado y ganasen dinero con ello.

- Empresas como Amazon Web Services, Azure de Microsoft, etc. Han ganado cientos de millones de dólares ofreciendo a sus clientes servicios basados en Software libre sin contribuir tanto a la comunidad de código abierto que construye y mantiene ese proyecto. Es imposible saber exactamente de cuánto dinero estamos hablando, pero es cierto que los proveedores de la nube se benefician del trabajo de los desarrolladores de código abierto que no emplean.

- Hay un mito ampliamente instalado en el mundo de código abierto que dice que los proyectos son impulsados por una comunidad de contribuyentes, pero en realidad, los desarrolladores pagados contribuyen con la mayor parte del código en la mayoría de los proyectos de código abierto modernos.

En resumen, todas estas voces se quejan de dos cosas: los grandes beneficios que obtienen los proveedores de servicios en la nube con su Software sin retribuirles en consecuencia, y la falta de colaboración manteniendo los productos con los que lucran. Sin embargo, no nos engañemos, el quid de la cuestión está principalmente en el dinero: la opinión generalizada de la

comunidad es que el Software de código abierto nunca fue pensado para que las empresas de servicios en la nube lo tomasen y lo vendieran.

Por otro lado, si es posible bifurcar un proyecto libre que se cierra, ¿no hubiese sido mejor colaborar con él antes y haber evitado el cierre? Si no se invierte y se mantiene con salud aquello que da beneficios, puede terminar por desaparecer. A medio camino entre el depredador y el parásito: así es como ven muchas desarrolladoras de código abierto a los proveedores de servicios en la nube.

Vale la pena retomar ahora la frase «el Software de código abierto nunca fue pensado para que las empresas de servicios en la nube lo tomasen y lo vendieran». ¿Para qué fue pensado el código abierto entonces? No hay ninguna licencia de código abierto o Software libre reconocida por la Free Software Foundation o la Open Source Initiative que prohíba hacer negocio con el Software. Lo que prohíben es la discriminación en la capacidad y alcance de su uso en función de la parte, se trate de un individuo o de la mayor multinacional imaginable.

¿Cuál es la solución a un embrollo de tamaña envergadura? Lo único claro es que no es una cuestión de blancos y negros y las consideraciones son demasiadas como para seguir ahondando: empresas que cotizan en bolsa quieren más dinero de otras compañías -que también cotizan en bolsa y por mucho más-, que además del Software ponen la infraestructura sobre la que distribuyen sus ofertas y que tienen la capacidad de clonar tu producto en un abrir y cerrar de ojos, no solo porque tienen el capital, sino porque tienen la experiencia necesaria tras contribuir técnica, pero también en muchos casos, económicamente, durante largo tiempo.

Pese a ello, esta situación está alterando el paradigma actual, en el que el modelo de desarrollo del código abierto se ha impuesto como impulsor de la innovación en el sector empresarial y ya hay quien habla de que nos acercamos al fin, o al principio del fin de la Era del Open Source, cuya preponderancia estaría sentenciada por la revolución de la nube, a la postre el mayor estímulo que haya tenido el código abierto hasta la fecha.

El futuro, pues, pasaría por el Shared Source Software, bajo el cual diferentes compañías con intereses alineados colaborarán en el desarrollo de proyectos concretos, pero limitando su explotación comercial a sí mismas. Todavía no estamos ahí, no obstante, y no parece tampoco que el relevo se vaya a dar en breve. De suceder, será muy llamativo: la muerte del código abierto por un éxito mal entendido.

11.5.4 El Código Abierto como Base de la Competitividad

En septiembre del 2021, se publicó un amplio y detallado informe llevado a cabo por el Fraunhofer ISI y por OpenForum Europe para la Comisión Europea, «The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy», cuantifica la importancia económica del código abierto aplicado tanto al Software como al Hardware, su efecto en la contribución al producto interior bruto generado, la reducción en aspectos como el coste total de propiedad, dependencia del proveedor y autonomía digital; lanza una serie de recomendaciones específicas de políticas públicas destinadas a lograr un sector público digitalmente autónomo, una investigación y desarrollo abierto que fomente el crecimiento europeo y una industria más digitalizada y competitiva.

En las estimaciones del informe se apunta que las empresas europeas invirtieron alrededor de mil millones de euros en Software de código abierto en 2018, lo que resultó en un impacto en la economía europea de entre 65,000 y 95,000 millones de euros. El análisis estima una relación costo-beneficio superior a 1:4 y predice que un aumento del 10% de las contribuciones de a repositorios de código abierto sería susceptible de generar anualmente entre un 0.4% y un 0.6% adicional en el PIB, así como más de seiscientas nuevas empresas tecnológicas en la Unión Europea.

El análisis de las contribuciones a repositorios de Software de código abierto en la Unión Europea revela que el ecosistema tiene una naturaleza diferente frente al norteamericano, con un volumen de contribuciones que provienen sobre todo de empleados de compañías pequeñas o muy pequeñas, frente a un escenario en los Estados Unidos en el que predominan grandes compañías tecnológicas que se benefician en sus modelos de negocio de la gran cantidad y de la rápida mejora del Software disponible. En Europa, los contribuyentes individuales ascendieron a más de 260,000, lo que representa el 8% de los casi 3.1 millones de empleados de la UE en el sector del desarrollo de Software en 2018. En total, los más de 30 millones de desarrollos consolidados en repositorios en los estados miembros de la Unión Europea representan una inversión de personal equivalente a casi mil millones de euros, que han pasado a estar disponibles en el dominio público y que, por lo tanto, no tienen que ser desarrollados por otros actores.

Según el análisis, cuanto más pequeña es la empresa, mayor es la inversión relativa en Software de código abierto (las empresas con 50 empleados o menos asumieron casi la mitad de los desarrollos en la muestra de las com-

pañías más activas). Aunque más del 50% de los contribuyentes pertenecen a la industria tecnológica (el 8% del total de sus empleados participaron en estos desarrollos), también hubo participación significativa de empresas de consultoría, científicas, técnicas y, en menor medida, de distribuidores, minoristas y empresas del ámbito financiero.

¿Puede una filosofía de desarrollo como el código abierto, disponible para todo el mundo, llegar a convertirse en una fuente de ventajas diferenciales para el resto de los países, que se ha visto tradicionalmente muy superado en su relevancia en el entorno tecnológico por los gigantes tecnológicos de Estados Unidos o de China? El informe afirma que su uso puede llegar a incidir en gran medida en el desarrollo de una independencia tecnológica superior, de una mayor competitividad y de más innovación. Veremos si llegamos a ver en el resto del mundo políticas que incentiven el uso del código abierto como una variable estratégica clave para ello. La idea, capitalizar la tecnología de una forma más orientada al procomún y al desarrollo colaborativo, suena sin duda atractiva e interesante.

11.5.5 Software Libre en Empresas y Corporaciones

En esta sección exploraremos algunas de las claves por las cuales el Software libre está hoy en el punto de mira de todo tipo de empresas y grandes corporaciones (algunas de las cuales ayer eran sus acérrimos enemigos). Pero hay que empezar destacando que corporativos como Google, Amazon Web Services, Azure de Microsoft, Microsoft, IBM, entre otras, en los últimos años han ganado miles de millones de dólares ofreciendo a sus clientes servicios y/o productos basados en Software libre y con una queja recurrente por su pobre o nula contribución a la comunidad de código abierto que construyó y mantiene esos proyectos.

Si bien es imposible saber exactamente de cuánto dinero estamos hablando, pero es cierto que empresas y corporaciones se benefician diariamente del trabajo de los desarrolladores de código abierto que no emplean.

Grandes Equipos de Programadores GNU/Linux ha demostrado que los equipos de desarrolladores grandes, distribuidos, aunque desorganizados pueden crear Software viable.

Antes de la llegada de GNU/Linux, la mayoría del Software era desarrollado por pequeños equipos de programadores que trabajaban en estrecha coordinación entre sí. Ese era el enfoque recomendado por informáticos de hace

unos decenios, que advertían que añadir más programadores a un proyecto tendía a disminuir su eficiencia. Y estaban muy equivocados.

Desde el principio, el Kernel de Linux se desarrolló con un enfoque diferente, en el que programadores de todo el mundo, que en la mayoría de los casos no se conocían, escribieron e integraron el código de forma rápida y poco organizada. Gracias a la publicación temprana y frecuente, consiguieron que funcionara y hoy día es el Kernel más usado en informática en supercomputadoras y dispositivos móviles.

Pero actualmente hay un mito ampliamente instalado en el mundo de código abierto, que dice que los proyectos son impulsados por una comunidad de contribuyentes gratuitos, pero en realidad, los desarrolladores pagados contribuyen con la mayor parte del código en la mayoría de los proyectos de código abierto modernos de los cuales las corporaciones pueden sacar provecho. Claro ejemplo es el propio Kernel de Linux, en el cual una gran cantidad de desarrolladores actuales pertenecen o son subvencionados por empresas, fundaciones o corporaciones (actualmente cientos de ellas), como en el caso de Linus Torvalds que trabaja bajo los auspicios de la Fundación de Linux.

Reutilización de Software Parte de la razón por la que Linux se hizo muy popular entre los ingenieros de Software con relativa rapidez fue que Linux -y el Software libre en general- facilita la reutilización del código escrito por otras personas.

Hoy en día, la reutilización de Software de terceros es habitual, incluso entre los equipos de desarrollo cuyos productos no son de código libre. Es difícil imaginar la construcción de una aplicación hoy en día sin hacer uso de las bibliotecas de Software de origen, las API de terceros u otros recursos externos a su propio proyecto.

Es cierto que proyectos como GNU, que precedió al Kernel de Linux en siete años, promovían la reutilización de código antes de que apareciera el núcleo. Pero, podría decirse que Linux fue el proyecto que trajo las prácticas de codificación libre a la corriente que tanto parece interesar a ciertas grandes empresas, ayudando a crear el modelo de ingeniería de Software de componentes de Software modulares y reutilizables.

Gestión Actual del Código Fuente Linus Torvalds, que creó el núcleo de Linux cuando era estudiante en Helsinki, es el más famoso por ese trabajo.

Pero un hecho a menudo olvidado es que Torvalds es también el padre de Git, el masivamente popular gestor de código fuente libre.

Torvalds creó Git para ayudar a gestionar el código fuente de Linux. Si Linux no existiera, tampoco existiría Git. Tampoco existiría GitHub, ni GitLab, ni GitOps. Y, lo que es más importante, sin la idea de Software libre y colaborativo de Richard Stallman, tampoco existiría la cultura de intercambio y colaboración abierta que sostienen estas tecnologías.

Estrategias de Despliegue de Software "App Store" Apple puede atribuirse el mérito de haber lanzado la primera App Store, un lugar donde los desarrolladores pueden compartir aplicaciones y los usuarios pueden instalarlas fácilmente, utilizando un catálogo Online centralizado.

Pero al igual que con muchas cosas que ha hecho Apple, el concepto de App Store (que ahora es una estrategia de despliegue de Software apilado como servicio, especialmente pero no sólo en el ecosistema móvil) se parece mucho a lo que los desarrolladores de GNU/Linux estaban haciendo a través de los repositorios de Software mucho antes de que las tiendas de aplicaciones se convirtieran en algo común en el mundo del Software propietario, como también lo es la Tienda de Windows.

Los repositorios de Software en GNU/Linux hacen más o menos lo mismo que las tiendas de aplicaciones: Permiten a los usuarios seleccionar las aplicaciones que quieren de una lista centralizada y en línea, y luego instalarlas con unos pocos clics o bien órdenes de terminal (como el famoso *apt* de Debian).

Es cierto que empresas como Apple parecen tener el mérito de crear tiendas de aplicaciones muy fáciles de usar de hacer clic e ir, pero no es un invento de ellos. Y la historia del concepto de tienda de aplicaciones en general implica a más actores que sólo la comunidad de Apple. Aún así, creo que se podría argumentar con fuerza que, sin GNU/Linux y los repositorios de Software de GNU/Linux, las tiendas de aplicaciones tal y como las conocemos hoy no existirían.

Formatos Abiertos para Intercambio de Información Hay una gran variedad de tecnologías disponibles para producir y almacenar datos. Como son: hojas de cálculo, bases de datos, Software estadístico más específico y más. Esto genera una enorme diversidad de formatos, a veces esto es por decir lo menos caótico.

La ventaja de los archivos de formatos abiertos, es que permiten a los de-

sarrolladores producir varios paquetes de Software y servicios utilizando esos formatos. Esto entonces reduce al mínimo los obstáculos para la reutilización de la información que contienen.

El advenimiento del Software libre ha generado algunos de los formatos abiertos más usados para el intercambio de información, pero los entes generadores de información no siempre se adecuan a los niveles de apertura deseados, algunos de estos formatos abiertos son: XML, JSON, YAML, RDF, REBOL, PDF, CSV, ODF, OOXML, TXT, HTML, HDF.

Pero, incluso si la información se proporciona en formato electrónico, formato legible por máquina y en detalle, puede existir problemas relacionados con el formato del archivo en sí (principalmente el generado por los diversos sistemas operativos). Los formatos en los cuales la información es publicada -en otras palabras, la base digital en la cual la información es almacenada- puede ser "abierta" o "cerrada".

Un formato abierto es aquel donde las especificaciones del Software están disponibles para cualquier persona, de forma gratuita, así cualquiera puede usar dichas especificaciones en su propio Software sin ninguna limitación en su reutilización que fuere impuesta por derechos de propiedad intelectual.

Si el formato del archivo es "cerrado", esto puede ser debido a que el formato es propietario y sus especificaciones no están disponibles públicamente, o porque el formato es propietario y aunque las especificaciones se han hecho públicas, su reutilización es limitada. Si la información es liberada en un formato de archivo cerrado, esto puede causar grandes obstáculos para reutilizar la información codificada en él, forzando a aquellos que deseen usar la información a comprar Software innecesario.

El uso de formatos de archivo con propiedad, para el que la especificación no está disponible públicamente, puede crear dependencia de Software de terceros o de los titulares de licencias de los formatos de archivos. En el peor de los casos, esto puede significar que la información sólo se puede leer con cierto Software específico, que puede ser caro, o que puede quedar obsoleto.

La preferencia del término Gobierno de Datos Abiertos, es que la información se publicará en formatos de archivo abiertos, los cuales son de lectura mecánica y esto es una aportación más del Software libre.

Ciencia Abierta La ciencia abierta (Open Science) es el movimiento creciente para hacer que la ciencia sea abierta. La ciencia en sí misma se utilizó como un ejemplo principal de la eficacia del movimiento de código abierto, ci-

tando prácticas como la difusión abierta de información, métodos y revisión por pares de la literatura científica. Podría decirse que la ciencia abierta comenzó en el siglo XVII con el advenimiento de la revista científica y la práctica de repetir los experimentos presentados en los artículos académicos. Estas revistas se imprimirían y distribuirían en todo el mundo, a menudo supervisadas por sociedades científicas como la Royal Society.

¿Qué impulsó la necesidad de un movimiento de ciencia abierta? La Royal Society tenía el famoso lema "Nullius in verba", traducido de forma aproximada como "no tome la palabra de nadie". Esto encarnaba un principio general en la ciencia de que todas las teorías están abiertas a ser cuestionadas y los resultados declarados deben ser repetibles. De hecho, es una práctica generalizada que fue realizada por la sociedad en esos primeros años. En los últimos años esta práctica no ha sido tan común, con más y más ciencia confiando en elementos cerrados, lo que en última instancia conduce a errores que son más difíciles de detectar sin un intercambio completo de información: datos, métodos y publicaciones.

El movimiento de ciencia abierta afirma en términos generales que la ciencia debe realizarse de manera abierta y reproducible donde todos los componentes de la investigación estén abiertos. Muchas revistas permanecen estancadas en un formato en el que se imprimían físicamente, a pesar de que en la actualidad se distribuyen en gran medida en línea. A menudo, todavía utilizan archivos PDF como una forma de "papel electrónico" con publicaciones fijas, procesos cerrados de revisión por pares y poco o ningún acceso a los datos. Este fue sin duda el modo más eficiente de difundir el conocimiento científico antes de los albores de internet, pero ahora un número cada vez mayor lo considera lejos de ser el óptimo.

La ciencia abierta encarna una serie de aspectos, en el núcleo esto incluye acceso abierto, datos abiertos, código abierto y estándares abiertos que ofrecen una diseminación sin restricciones del discurso científico. Estas cosas permiten una ciencia reproducible al brindar acceso completo a los componentes principales de la investigación científica. Hay una serie de componentes adicionales que también se están explorando, como la revisión por pares abierta, donde los revisores de publicaciones científicas publican revisiones abiertamente con su nombre adjunto y la ciencia de libreta abierta donde las libretas (tradicionalmente cerradas) se publican abiertamente en línea a medida que se realiza la investigación.

¿Por qué la ciencia abierta es tan importante en la era digital? También existe una creciente comprensión de que, dado que la investigación científica

depende cada vez más del código informático para simulaciones, cálculos, análisis, visualización y procesamiento de datos en general, es importante tener acceso a este código tal como tradicionalmente ha sido importante mostrar (y derivar) cualquier nueva técnica matemática introducida para el análisis. Hay revistas como PLOS ONE y F1000 que exploran el significado de las publicaciones, ya sea que se deben congelar en el tiempo o se pueden actualizar. Los repositorios de datos también están ganando importancia a medida que las agencias de financiación requieren la publicación y preservación de los datos generados por la investigación financiada.

En esencia, la ciencia abierta se trata de volver a esos valores fundamentales inculcados por algunos de los primeros científicos de que no debemos confiar en la palabra de nadie, que es esencial que todos los elementos pertinentes a un descubrimiento pretendido se publiquen para que los resultados puedan repetirse y validarse. El movimiento de la ciencia abierta varía en el grado en que lo requiere, pero están surgiendo patrones. Se están estableciendo recomendaciones sobre licencias, como CC0 para datos, CC-BY para publicaciones, licencias compatibles con OSI para código fuente y formatos abiertos para datos. En última instancia, se trata de empoderar a todos para que participen en la ciencia, con internet como vehículo principal para la amplia difusión de este conocimiento.

Este movimiento está cambiando la forma en que se hace la ciencia, está recibiendo el respaldo de muchas agencias de financiamiento, ya que requieren planes de gestión de datos, planes de distribución de código fuente y una mayor validación de los resultados a través del acceso abierto a estos resultados para todos. Esto también mejora la transferencia de conocimientos de la academia a la industria, ya que se brinda acceso completo en el momento de la publicación o después de un período de embargo. El movimiento de la ciencia abierta se limita en gran medida a la investigación que está financiada por las agencias de financiación nacionales de todo el mundo y exige que todos los que financian la investigación tengan acceso total e igualitario a ella.

Open Hardware El concepto de Software libre también se permeó al Hardware. El término Open Hardware u Open Source Hardware, se refiere al Hardware cuyo diseño se hace públicamente disponible para que cualquiera pueda estudiarlo, modificarlo y distribuirlo, además de poder producir y vender Hardware basado en ese diseño. Tanto el Hardware como el Software

que lo habilita, siguen la filosofía del Software libre. Hoy en día, el término "hágalo usted mismo" (DIY por sus siglas en inglés) se está popularizando en el Hardware gracias a proyectos como Arduino que es una fuente abierta de prototipos electrónicos, una plataforma basada en Hardware flexible y fácil de utilizar que nació en Italia en el año 2005.

El movimiento de Hardware abierto o libre, busca crear una gran librería accesible para todo el mundo, lo que ayudaría a las compañías a reducir en millones de dólares en trabajos de diseño redundantes. Ya que es más fácil tener una lluvia de ideas propuesta por miles o millones de personas, que por solo una compañía propietaria del Hardware, tratando así de que la gente interesada entienda cómo funciona un dispositivo electrónico, pueda fabricarlo, programarlo y poner en práctica esas ideas en alianza con las empresas fa-bricantes, además se reduciría considerablemente la obsolescencia programada y en consecuencia evitaríamos tanta basura electrónica que contamina el medio ambiente. Al hablar de Open Hardware hay que especificar de qué tipo de Hardware se está hablando, ya que está clasificado en dos tipos:

- Hardware estático. Se refiere al conjunto de elementos materiales de los sistemas electrónicos (tarjetas de circuito impreso, resistencias, capacitores, LEDs, sensores, etcétera).

- Hardware reconfigurable. Es aquél que es descrito mediante un HDL (Hardware Description Language). Se desarrolla de manera similar a como se hace Software. Los diseños son archivos de texto que contienen el código fuente.

Para tener Hardware reconfigurable debemos usar algún lenguaje de programación con licencia GPL (General Public License). La licencia GPL, al ser un documento que cede ciertos derechos al usuario, asume la forma de un contrato, por lo que usualmente se le denomina contrato de licencia o acuerdo de licencia. La Organización Europea para la investigación Nuclear (CERN) publicó el 8 de julio de 2011 la versión 1.1 de la Licencia de Hardware Abierto.

Existen programas para diseñar circuitos electrónicos y aprender de la electrónica como EDA (Electronic Design Automation) y GEDA (GPL Electronic Design Automation), son aplicaciones de Software libre que permiten poner en práctica las ideas basadas en electrónica.

Es posible realizar el ciclo completo de diseño de Hardware reconfigurable desde una máquina con GNU/Linux, realizándose la compilación, simulación,

síntesis y descarga en una FPGA (Field Programmable Gate Arrays). Para la compilación y simulación se puede usar GHDL (https://ghdl.free.fr) junto con GTKWave (https://gtkwave.sourceforge.net) y para la síntesis el entorno ISE de Xilinx. Este último es Software comercial pero existe una versión gratuita con algunas restricciones.

Sabemos que tanto en el caso del Software como el Hardware, libre no es lo mismo que gratis. Específicamente, en el caso del Hardware, como estamos hablando de componentes físicos que son fabricados, la adquisición de componentes electrónicos puede ser costosa. Aun así, es un campo que no solo es apasionante sino que también tiene mucho futuro y representa grandes oportunidades.

Entusiasmo de la Comunidad Por último, pero no menos importante, probablemente el mayor impacto duradero de GNU/Linux en el modelo de ingeniería de Software se reduce a lo que podría llamarse entusiasmo de la comunidad. Me refiero a la forma en que GNU/Linux en particular, y el Software libre en general, ha animado a los desarrolladores de todo tipo a considerar las contribuciones a la comunidad como uno de sus objetivos finales y esto ahora es notorio no solo en Software, sino en Hardware abierto, obras literarias, escritos técnicos (como este trabajo), imágenes, vídeo, música y un largo etc.

En un mundo de código libre en el que las contribuciones a los proyectos de código pueden ser aceleradores de carrera y el código de licencia libre se reutiliza ampliamente, los desarrolladores entienden que hay un valor real en la construcción de Software que puede beneficiar a tantos usuarios como sea posible.

Tal vez los desarrolladores valorarían a la comunidad en su conjunto si GNU/Linux y el código libre nunca hubieran aparecido. Pero me cuesta imaginar un mundo en el que corporaciones como Microsoft y Google trabajarán juntos en la construcción de Software para GNU/Linux si GNU/Linux no hubiera popularizado el concepto de proyectos de Software impulsados por la comunidad que nadie posee realmente, pero que todos pueden utilizar.

Si bien, es innegable que todo lo anterior puso en la mira de las empresas de todos los tamaños y de las grandes corporaciones el Software libre, la principal razón es el poder utilizar una gran cantidad Software funcional, depurado y ampliamente usado para ofrecer servicios y/o productos basados en Software libre y así beneficiarse económicamente de ello.

Por otro lado, se ha visto a través de múltiples estudios, el impacto y la cuantificación de la importancia económica del código abierto aplicado tanto al Software como al Hardware, su efecto en la contribución al producto interior bruto generado, la reducción en aspectos como el coste total de propiedad, dependencia del proveedor y autonomía digital. Además de generar políticas públicas destinadas a lograr un sector público digitalmente autónomo, una investigación y desarrollo abierto que fomente el crecimiento de los países y una industria más digitalizada y competitiva.

Retomando la frase «el Software de código abierto nunca fue pensado para que las empresas de servicios lo tomasen y lo vendieran». ¿Para qué fue pensado el código abierto, entonces? No hay ninguna licencia de código abierto o Software libre reconocida por la Free Software Foundation o la Open Source Initiative que prohíba hacer negocio con el Software. Lo que prohíben es la discriminación en la capacidad y alcance de su uso en función de la parte, se trate de un individuo o de la mayor multinacional imaginable.

Pese a ello, esta situación está alterando el paradigma actual, en el que el modelo de desarrollo del código abierto se ha impuesto como impulsor de la innovación en el sector empresarial, a la postre el mayor estímulo que haya tenido el código abierto hasta la fecha.

¿Puede una filosofía de desarrollo como el código abierto, disponible para todo el mundo, llegar a convertirse en una fuente de ventajas diferenciales para el resto de los países, que se ha visto tradicionalmente muy superado en su relevancia en el entorno tecnológico por los gigantes tecnológicos de Estados Unidos o de China? Se afirma que su uso puede llegar a incidir en gran medida en el desarrollo de una independencia tecnológica superior, de una mayor competitividad y de más innovación. La idea, capitalizar la tecnología de una forma más orientada al procomún y al desarrollo colaborativo, suena sin duda atractiva e interesante pero no libre de inconvenientes para algunos sectores de desarrolladores de Software libre.

11.6 Código Abierto y las Organizaciones Internacionales

Aunque la Organización de las Naciones Unidas (ONU) ha hablado previamente bien del desarrollo del código abierto, varios eventos recientes muestran que la ONU está tomando medidas definitivas para presentar al mundo entero el camino del código abierto. En julio del 2021, el Consejo Económico y Social de la ONU (ECOSOC) adoptó un proyecto de resolución presentado por el representante de Pakistán titulado: Tecnologías de fuente abierta para

el desarrollo sostenible.

11.6.1 Las Naciones Unidas y el Código Abierto

El ECOSOC destacó la disponibilidad de tecnologías de código abierto que pueden contribuir a los Objetivos de Desarrollo Sostenible (ODS). El consejo invitó al Secretario General a "desarrollar propuestas específicas sobre formas de aprovechar mejor las tecnologías de código abierto para el desarrollo sostenible basadas en las aportaciones de los Estados Miembros interesados y otras partes interesadas".

El desarrollo de tecnología de código abierto puede ser una herramienta rápida y eficaz para la innovación. Aplicarlo a tecnologías apropiadas para ayudar a alcanzar los ODS es extremadamente prometedor. Las "tecnologías apropiadas" abarcan opciones y aplicaciones tecnológicas que son a pequeña escala, económicamente asequibles, descentralizadas, energéticamente eficientes, ambientalmente racionales y fácilmente utilizadas por las comunidades locales para satisfacer sus necesidades.

Existe un caso particularmente fuerte para las tecnologías apropiadas de código abierto OSAT (Outsourced Semiconductor Assembly and Test). OSAT podría ayudar a todos a salir de la pobreza y alcanzar un estado sostenible aprovechando el mismo tipo de desarrollo que hace que el Software de código abierto sea un éxito rotundo.

La Declaración Ministerial del Foro político de alto nivel sobre desarrollo sostenible también destacó la importancia de "tecnologías no patentadas que pueden contribuir a los Objetivos de Desarrollo Sostenible, a través de diversas fuentes de acceso abierto". Pidió "el desarrollo y la puesta en funcionamiento de una plataforma en línea en el marco del Mecanismo de facilitación de la tecnología para establecer un mapeo integral y servir como puerta de entrada a la información sobre iniciativas, mecanismos y programas de ciencia, tecnología e innovación existentes, dentro y fuera de las Naciones Unidas".

Es un pequeño paso, pero muy emocionante, porque las Naciones Unidas no se demoran una vez que ven formas de ayudar a sus Estados Miembros y a las personas que los integran. Ahora, el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas (DESA) está trabajando para que esto suceda. DESA está utilizando una Nota sobre una base de datos centralizada propuesta de las Naciones Unidas de tecnologías apropiadas de código abierto publicada por la Conferencia de las Naciones Unidas sobre Comercio

y Desarrollo (UNCTAD) para hacerlo.

La Nota de la UNCTAD aboga por una base de datos centralizada de OSAT para acelerar el descubrimiento y la innovación en todos los sectores asociados con los ODS al tiempo que se minimizan los obstáculos legales o financieros. Esto es importante para la difusión del acervo mundial de conocimientos, especialmente en los países en desarrollo.

Actualmente, no existe un repositorio completo o una base de datos central de OSAT y Appropedia.org, quizás sea el mejor ejemplo. Sin embargo, la Nota de la UNCTAD dice: "Muchas organizaciones, organizaciones sin fines de lucro y empresas con fines de lucro están desarrollando OSAT y manteniendo bases de datos existentes a pequeña escala. Si bien hay muchos OSAT disponibles, se encuentran dispersos en varias bases de datos para tecnologías particulares. Mientras tanto, sigue existiendo una clara necesidad de aumentar la tasa de uso de OSAT.

Por lo tanto, existe una necesidad urgente de una base de datos de código abierto centralizada global (COSD) confiable. Al tener un alcance global, un repositorio de COSD proporcionaría una ventanilla única a la que todos pueden acceder para resolver los desafíos locales".

Concluye: "La ONU está bien posicionada para liderar el establecimiento de un COSD dado su papel bien establecido en la promoción de la tecnología de código abierto a través de varios foros y publicaciones intergubernamentales. En particular, 2030 Connect es una plataforma tecnológica en línea de la ONU que se desarrolló como parte del trabajo del Equipo de Trabajo Interinstitucional de la ONU. El COSD podría mejorarlo".

Con el liderazgo de la ONU, quizás no estemos demasiado lejos de cuándo, sí tiene un problema local (sin importar en qué parte del mundo se encuentre), pueda descargar una solución de código abierto examinada y probada. Quizás, esta es la potencia de fuego que necesitamos para alcanzar los ambiciosos Objetivos de Desarrollo Sostenible.

11.6.2 La Comisión Europea se Compromete a Liberar Todo el Software que Pueda Beneficiar a la Sociedad

A finales del 2021, la Unión Europea (UE) y su órgano legislativo, la Comisión Europea siguen avanzando en su estrategia digital con el Software de código abierto como uno de los pilares fundamentales. En esta ocasión ha sido esta última la que anuncia novedades para con la distribución del Software desarrollado para cubrir necesidades internas de la organización.

De acuerdo a la información publicada, la Comisión Europea ha aprobado una nueva regulación que favorece el libre acceso al Software que producen siempre y cuando existan beneficios potenciales para «los ciudadanos, las empresas u otros servicios públicos», lo que de la teoría a la práctica bien puede abarcar todo lo que se desarrolle bajo su tejado.

Esta nueva disposición se apoya a su vez en un reciente estudio realizado también por la Comisión sobre el impacto del Software de código abierto en áreas como la independencia tecnológica, la competitividad y la innovación en la economía de la Unión Europea. El objetivo, hallar evidencias sólidas con las que conformar las políticas europeas de código abierto para los próximos años.

En términos económicos, de hecho, los cálculos son de lo más optimistas y apuntan un impacto económico contundente, de miles de millones de euros de ahorro al año -a modo de ejemplo, se estimó entre 65 y 95 mil millones de euros solo en 2018- y con un incremento mínimo en la apuesta, se podría dar un crecimiento del PIB de la UE de en torno a los 100,000 millones de euros.

Con semejante escenario, no es de extrañar que la misma Comisión Europea esté interesada en promover las soluciones de código abierto dentro y fuera de las instituciones y no solo se basan en el beneficio económico directo: son muchas otras las ventajas del modelo también recogidas en el informe, tal y como se ha mencionado: independencia, competitividad, innovación... y en el caso de las administraciones públicas, colaboración, reutilización y transparencia.

En palabras de Johannes Hahn, comisario de Presupuesto y Administración: «El código abierto ofrece grandes ventajas en un ámbito en el que la UE puede desempeñar un papel de liderazgo. Las nuevas normas aumentarán la transparencia y ayudarán a la Comisión, así como a los ciudadanos, las empresas y los servicios públicos de toda Europa, a beneficiarse del desarrollo de Software de código abierto. Poner en común los esfuerzos para mejorar el Software y la creación conjunta de nuevas funciones reduce los costes para la sociedad, ya que también nos beneficiamos de las mejoras realizadas por otros desarrolladores. Esto también puede mejorar la seguridad, ya que especialistas externos e independientes comprueban los fallos y las deficiencias de seguridad de los programas informáticos».

La comisaría de Innovación, Investigación, Cultura, Educación y Juventud, Mariya Gabriel, ha declarado: «La Comisión pretende, con su ejemplo, estar al frente de la transición digital en Europa. Con las nuevas normas, la

Comisión aportará un valor significativo a las empresas, también las emergentes, a los innovadores, a los ciudadanos y las administraciones públicas, poniendo a su disposición el código abierto de sus soluciones informáticas. Esta decisión también ayudará a estimular la innovación, gracias al código de la Comisión disponible públicamente».

Como muestra del Software desarrollado bajo el amparo de la Comisión Europea que va a ser liberado se incluyen proyectos como eSignature, «un conjunto de normas, herramientas y servicios gratuitos que ayudan a las administraciones públicas y a las empresas a acelerar la creación y verificación de firmas electrónicas jurídicamente válidas en todos los Estados miembros de la UE»; o LEOS (Legislation Editing Open Software), «el Software utilizado en toda la Comisión para elaborar textos jurídicos. LEOS, escrito originalmente para la Comisión, se está desarrollando en estrecha colaboración con Alemania, España y Grecia».

Esta nueva iniciativa de la Comisión Europa contempla asimismo la creación de un repositorio centralizado para facilitar el descubrimiento, el acceso y la reutilización del Software incluido, el cual se sumará a todos los proyectos realizados por las diferentes administraciones públicas comunitarias en base al mismo modelo de desarrollo. Y viene de lejos este impulso, aun cuando comienza a unificarse ahora.

Sin ir más lejos, hace años que la propia Comisión Europea puso en marcha el programa Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens que dio origen al observatorio JoinUp (https://joinup.ec.europa.eu/), en cuyas páginas se recogen casi 3,000 soluciones de Software abierto, 133 colecciones de recursos y cuantiosa información relacionada.

Más tarde, de 2014 a 2017 se inició la «primera fase» en la estrategia de código abierto de la Unión Europea, especialmente dentro de la propia Comisión, estableciendo determinados requisitos en materia de Software de código abierto; actualmente se está desarrollando la nueva «estrategia de código abierto 2020-2023», con la que la Comisión Europea pretende ampliar y afianzar los objetivos de la estrategia digital y la contribución al programa Europa Digital.

12 Apéndice B: Máquinas Virtuales

Entendamos por una máquina virtual a un programa de cómputo (véase [19], [20], [17] y [16]) que simula a una computadora, en la cual se puede instalar y usar otros sistemas operativos de forma simultánea como si fuese una computadora real sobre nuestro sistema operativo huésped[110].

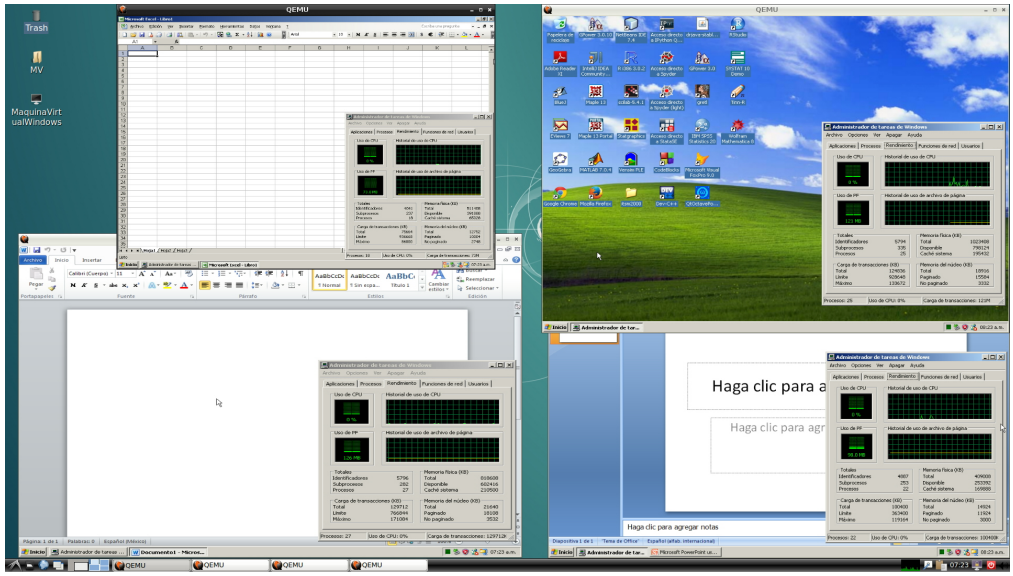

Figura 1: Sobre un equipo AMD de gama baja y 4 GB de RAM, usando como sistema operativo huésped un Linux Debian estable, se ejecutan 4 máquinas virtuales (mediante KVM) de Windows XP con diferentes aplicaciones y dentro de cada una de ellas se muestra la RAM asignada, la usada en ese momento, el uso de CPU de cada máquina virtual, entre otros datos.

Una característica esencial de las máquinas virtuales es que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados por ellas. Estos procesos no pueden escaparse de esta "computadora virtual". Uno de los usos más extendidos de las máquinas virtuales es ejecutar sistemas operativos nuevos u obsoletos adicionales a nuestro sistema habitual.

[110] Tal y como puede verse reflejado en la definición de máquina virtual, en este texto nos estamos focalizando en las máquinas virtuales de sistema. Existen otro tipo de máquinas virtuales, como por ejemplo las máquinas virtuales de proceso o los emuladores.

De esta forma podemos ejecutar uno o más sistemas operativos -Linux, Mac OS, Windows XP, 7 ó 8- desde nuestro sistema operativo habitual -GNU/Linux, Unix o Windows- sin necesidad de instalarlo directamente en nuestra computadora y sin la preocupación de que se desconfigure el sistema operativo huésped o a las vulnerabilidades del sistema virtualizado, ya que podemos aislarlo para evitar que se dañe.

12.1 Tipos de Máquinas Virtuales

Las máquinas virtuales se pueden clasificar en dos grandes categorías según su funcionalidad y su grado de equivalencia a una verdadera máquina:

- Máquinas virtuales de sistema (en inglés System Virtual Machine). También llamadas máquinas virtuales de Hardware[111], permiten a la má-quina física subyacente compartirse entre varias máquinas virtuales, cada una ejecutando su propio sistema operativo[112]. A la capa de Software que permite la virtualización se le llama monitor de máquina virtual o Hypervisor. Un monitor de máquina virtual puede ejecutarse o bien directamente sobre el Hardware o bien sobre un sistema operativo ("Host Operating System").

- Máquinas virtuales de proceso (en inglés Process Virtual Machine). A veces llamada "máquina virtual de aplicación", se ejecuta como un proceso normal dentro de un sistema operativo y soporta un solo proceso. La máquina se inicia automáticamente cuando se lanza el proceso que se desea ejecutar y se detiene para cuando éste finaliza. Su objetivo es el de proporcionar un entorno de ejecución independiente de la plataforma de Hardware y del sistema operativo, que oculte los detalles de la plataforma subyacente y permita que un programa se ejecute siempre de la misma forma sobre cualquier plataforma.

[111] La virtualización puede se por Software o con apoyo mediante el Hardware, en este último caso se obtienen varios órdenes de magnitud de rendimiento que por Software.

[112] Que sus componentes sean virtuales no quiere decir necesariamente que no existan, por ejemplo una máquina virtual puede tener unos recursos reservados de 2 GB de RAM y 20 GB de disco que se obtienen del equipo donde este ejecutando la máquina virtual. Otros dispositivos podrían realmente ser inexistentes físicamente como por ejemplo un CD-ROM que en verdad es el contenido de una imagen ISO en vez de un lector de CD de verdad.

12.2 Técnicas de Virtualización

Las Máquinas Virtuales ya tienen más de 60 años de vida su origen en los primeros días de la informática en la década de 1960, cuando el tiempo compartido para los usuarios de la computadora central era un medio de separar el Software de un sistema anfitrión físico. La máquina virtual se definió a principios de los 70 como "un duplicado eficiente y aislado de una máquina de computación real".

Las máquinas virtuales tal como las conocemos hoy en día han cobrado fuerza en los últimos 20 años a medida que las empresas adoptaron la virtualización de servidores para utilizar la potencia de computación de sus servidores físicos de manera más eficiente, reduciendo la necesidad de servidores físicos y ahorrando así espacio en el centro de datos. Debido a que las aplicaciones con diferentes requisitos de sistema operativo podían funcionar en un solo Host físico, no se requería un Hardware de servidor diferente para cada una.

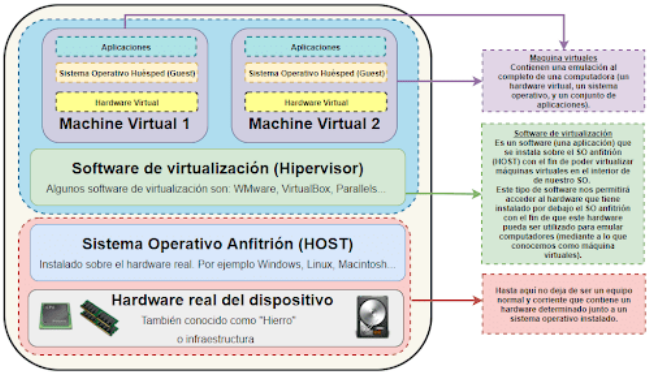

Figura 2: Qué es una Máquina Virtual

Básicamente se reconocen tres tipos de virtualización, algunas de las cuales son usadas actualmente en la gran mayoría de los sistemas operativos, ge-neralmente sin que el usuario esté consciente de que usa virtualización[113], estos son:

[113] El ejemplo más común y omnipresente es la máquina virtual del lenguaje de programación de JAVA o .Net Framework.

Emulación del Hardware Subyacente (ejecución nativa) Esta técnica se suele llamar virtualización completa -Full Virtualization- del Hardware, y se puede implementar usando un Hipervisor de Tipo I o de Tipo II:

1. Monitor de tipo I, se ejecuta directamente sobre el Hardware.
2. Monitor de tipo II, se ejecuta sobre otro sistema operativo.

Cada máquina virtual puede ejecutar cualquier sistema operativo soportado por el Hardware subyacente. Así los usuarios pueden ejecutar dos o más sistemas operativos distintos simultáneamente en computadoras "privadas" virtuales. Actualmente tanto Intel como AMD han introducido prestaciones a sus procesadores x86_64 para permitir la virtualización de Hardware.

Emulación de un Sistema no Nativo Las máquinas virtuales también pueden actuar como emuladores de Hardware, permitiendo que aplicaciones y sistemas operativos concebidos para otras arquitecturas de procesador se puedan ejecutar sobre un Hardware que en teoría no soportan. Esta técnica permite que cualquier computadora pueda ejecutar Software escrito para la máquina virtual. Sólo la máquina virtual en sí misma debe ser portada a cada una de las plataformas de Hardware.

Virtualización a Nivel de Sistema Operativo Esta técnica consiste en dividir una computadora en varios compartimentos independientes de manera que en cada compartimento podamos instalar un servidor. A estos compartimentos se les llama "entornos virtuales". Desde el punto de vista del usuario, el sistema en su conjunto actúa como si realmente existiesen varios servidores ejecutándose en varias máquinas distintas.

12.3 Otras Formas de Virtualización

El éxito de las máquinas virtuales en la virtualización de servidores llevó a aplicar la virtualización a otras áreas, como son el almacenamiento, las redes o las computadoras de escritorio. Lo más probable es que, si hay un tipo de Hardware que se está utilizando en el centro de datos, se esté explorando el concepto de virtualizarlo.

Virtualización de escritorios Implementar los escritorios como un servicio gestionado permite a las organizaciones de tecnología de la información responder más rápido a las necesidades cambiantes del entorno de trabajo y a las nuevas oportunidades. Los escritorios y las aplicaciones virtualizados también pueden distribuirse de forma rápida y sencilla a sucursales, empleados subcontratados o en otros países y trabajadores móviles que utilizan dispositivos móviles como tabletas iPad y Android.

Virtualización de redes las empresas han explorado opciones de red como servicio y la virtualización de funciones de red -NFV, Network Functions Virtualization-, que utiliza servidores de productos básicos para sustituir los aparatos de red especializados y permitir servicios más flexibles y escalables. Esto difiere un poco de la red definida por los programas informáticos, que separa el plano de control de la red del plano de reenvío para permitir un aprovisionamiento más automatizado y una gestión de los recursos de la red basada en políticas.

Una tercera tecnología, las funciones de red virtual, son servicios basados en programas informáticos que pueden ejecutarse en un entorno NFV, incluidos procesos como el enrutamiento, el cortafuegos, el equilibrio de la carga, la aceleración de la WAN y el cifrado.

Máquinas Virtuales y Contenedores El crecimiento de las máquinas virtuales ha dado lugar a un mayor desarrollo de tecnologías como los contenedores, que llevan el concepto un paso más allá y está ganando atractivo entre los desarrolladores de aplicaciones Web. En el entorno de un contenedor, una sola aplicación, junto con sus dependencias, puede ser virtualizada. Con muchos menos gastos generales que una máquina virtual, un contenedor sólo incluye binarios, bibliotecas y aplicaciones.

Mientras que algunos piensan que el desarrollo de contenedores puede "matar" a la máquina virtual, hay suficientes capacidades y beneficios de las máquinas virtuales que mantienen la tecnología en movimiento. Por ejemplo, las máquinas virtuales siguen siendo útiles cuando se ejecutan múltiples aplicaciones juntas o cuando se ejecutan aplicaciones heredadas en sistemas operativos más antiguos.

Además, algunos opinan que los contenedores son menos seguros que los hipervisores de las máquinas virtuales porque los contenedores tienen un solo sistema operativo que las aplicaciones comparten, mientras que las máquinas

virtuales pueden aislar la aplicación y el sistema operativo.

Máquinas Virtuales, 5G y Edge Computing Las máquinas virtuales son vistas como parte de nuevas tecnologías como el 5G y el Edge Computing. Por ejemplo, los proveedores de infraestructura de escritorio virtual -VDI, Virtual Desktop Infrastructure- como Microsoft, VMware y Citrix están buscando formas de extender sus sistemas VDI a los empleados que ahora trabajan en casa a causa de la pandemia.

Como muchas otras tecnologías que se utilizan hoy en día, éstas no se habrían desarrollado si no fuera por los conceptos originales de máquinas virtuales introducidos hace décadas.

12.4 Aplicaciones de las Máquinas Virtuales de Sistema

Cada uno de los sistemas operativos que virtualizamos -con su propio sistema operativo llamado sistema operativo «invitado (Guest)»- es independiente de los otros sistemas operativos. De este modo, en caso que una de las máquinas virtuales deje de funcionar, el resto seguirá funcionando. Una máquina virtual dispone de todos los elementos de un equipo de cómputo real, de disco duro, memoria RAM, unidad de CD o DVD, tarjeta de red, tarjeta de vídeo, etc., pero a diferencia de un equipo de cómputo real estos elementos en vez de ser físicos son virtuales. Así, una vez instalado un sistema operativo en la máquina virtual, podemos usar el sistema operativo virtualizado del mismo modo que lo usaríamos si lo hubiéramos instalado en nuestro equipo de cómputo.

Varios sistemas operativos distintos pueden coexistir sobre la misma computadora trabajando simultáneamente, en sólido aislamiento el uno del otro, por ejemplo para probar un sistema operativo nuevo sin necesidad de instalarlo directamente. La máquina virtual puede proporcionar una arquitectura de instrucciones que sea algo distinta de la verdadera máquina, es decir, podemos simular Hardware. Además, todos los elementos de una máquina virtual se encapsulan en un conjunto pequeño de archivos -en KVM/QEMU es solo un archivo-, esto permite que podamos pasar un sistema operativo virtual de un equipo de cómputo a otro y realizar copias de seguridad de forma fácil y rápida.

La gran mayoría de los manejadores de máquinas virtuales -KVM, Vir-

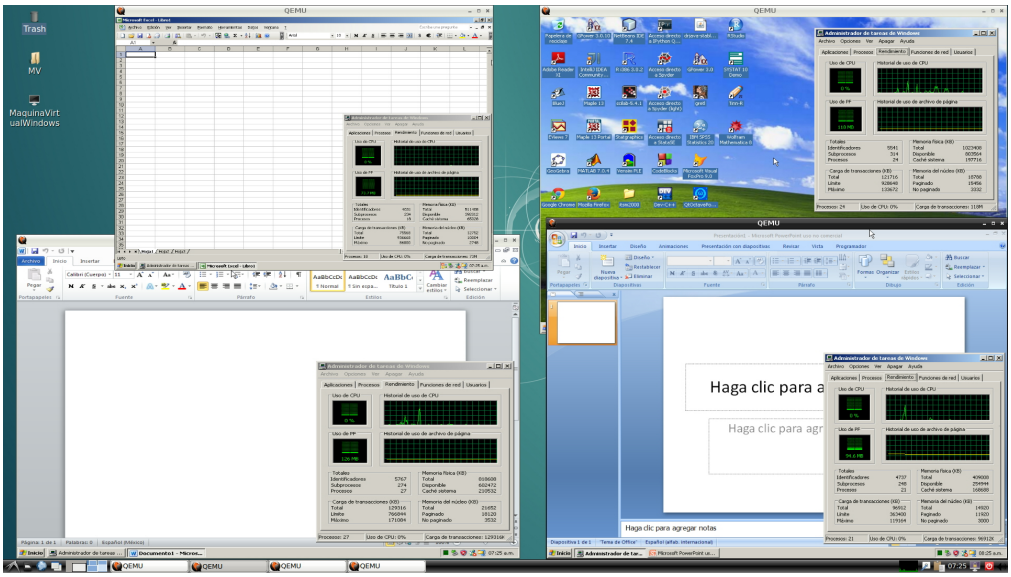

Figura 3: Al poder correr diferentes sistemas operativos y/o versiones del mismo en donde podemos instalar diversas aplicaciones antagónicas que no podrían coexistir en un sólo sistema operativo, nos permite ampliar el uso de nuestro equipo de cómputo.

tualBox o VMWare- permiten instalar prácticamente cualquier sistema operativo -por ejemplo Linux, Android, Mac OS X, Windows, Chrome OS, etc.-. Sin embargo existen otros manejadores de máquinas virtuales -Virtual PC, Hiper-V o Parallels- que están principalmente destinados a virtualizar Windows.

La virtualización es una excelente opción hoy en día, ya que las máquinas actuales -Laptops, Desktops y servidores- en la mayoría de los casos están siendo "subutilizados" -estos cuentan con una gran capacidad de cómputo, disco duro y memoria RAM- ya que no se utilizan todos los recursos todo el tiempo, teniendo un uso promedio que oscila entre 30% a 60% de su capacidad total. Permitiendo así, ejecutar varias máquinas virtuales en un sólo equipo físico aumentando el porcentaje de uso de los recursos de cómputo disponibles -en el caso de virtualizar servidores, a este proceso se le conoce como consolidación de servidores-. Así, la consolidación de servidores contribuye a reducir el coste total de las instalaciones necesarias para mantener los servicios, permitiendo un ahorro considerable de los costos asociados -

energía, mantenimiento, espacio, administración, etc.-, esto se hace patente en la «computación en la nube (Cloud Computing)» muy en boga actualmente.

12.5 Ventajas y Desventajas

Como toda tecnología, la virtualización tiene ventajas y desventajas, las cuales deben de ser sopesadas en cada ámbito de implementación. Lo que es un hecho que permite en un mismo equipo de cómputo ejecutar más de un sistema operativo o distintas versiones del mismo.

Pero queda claro que uno de los inconvenientes de las máquinas virtuales, es que agregan gran complejidad al sistema en tiempo de ejecución. Esto tiene como efecto la ralentización del sistema, es decir, el programa no alcanzará la misma velocidad de ejecución que si se instalase directamente en el sistema operativo «anfitrión (Host)» o directamente sobre la plataforma de Hardware, sin embargo, a menudo la flexibilidad que ofrecen compensa esta pérdida de eficiencia.

Si la virtualización es por Hardware, la velocidad de ejecución es más que aceptable para la mayoría de los casos, por ejemplo, en el caso de usar KVM/QEMU soporta máquinas virtuales de hasta 255 CPUs y 4 TB de RAM, y el rendimiento de aplicaciones como Oracle, SAP, LAMP, MS Exchange sobre máquinas virtuales puede oscilar entre el 95% y el 135% comparado con su ejecución en servidores físicos. Además, se ha conseguido ejecutar hasta 600 máquinas virtuales en un solo servidor físico.

12.5.1 Ventajas

Además de permitir ejecutar múltiples sistemas operativos, diferentes versiones de un mismo sistema pero con diferente Software que en principio puede ser incompatible entre sí. Para usuarios de Windows, el hecho en sí, de no tener porque lidiar con problemas derivados de virus y antivirus le confiere una gran ventaja desde el punto de vista administrativo y del usuario final. Además, permite una administración centralizada, ya que todas las máquinas virtuales tendrían la misma configuración y paquetes sin importar el Hardware subyacente en las que se ejecute el sistema operativo huésped.

En el caso de instituciones educativas de cualquier nivel académico, es común que en un mismo equipo de cómputo sea necesario ejecutar por un lado diferentes versiones de sistemas operativos -por ejemplo Linux, Windows XP,

Windows 7, etc.- y por otro lado, en un sistema operativo, ejecutar diferentes versiones de un mismo paquete -generalmente no se pueden tener instalados simultáneamente más de una versión-.

Las máquinas virtuales son una verdadera opción para coexistir simultáneamente diferentes versiones de sistemas operativos y en un mismo sistema máquinas virtuales ejecutando las diversas versiones de un mismo programa de cómputo, además se pueden configurar para que al momento de iniciarlas siempre se ejecuten a partir de una configuración e instalación base, de tal forma que al ser lanzadas, el usuario pueda instalar, configurar e inclusive dañar la máquina virtual, pero al reiniciarse la máquina virtual en una nueva sesión, se regresa a la configuración de la versión base, de esta forma no hay posibilidad de infección de virus entre diversos lanzamientos de sesiones de la máquina virtual, la actualización es centralizada y se puede hacer por red, sin intervención del usuario.

Por ello, es una opción viable y común tener en una máquina un sistema huésped como Debian GNU/Linux Estable y dentro de él, un grupo de máquinas virtuales de Windows -Windows XP, Windows 7, etc.-, en los que cada máquina virtual tenga instalado Software agrupado por las características del sistema operativo necesario para ejecutar a todas las aplicaciones seleccionadas -por ejemplo agrupados por la versión de Service Pack-.

Por otro lado, si se desconfigura un sistema operativo virtualizado es sumamente fácil de restaurar si lo comparamos con una máquina real. Si tomamos las precauciones necesarias podemos restaurar el estado que tenía un sistema operativo virtualizado, de forma fácil y rápida. Si hablamos del entorno empresarial, la virtualización de sistemas operativos supone un ahorro económico y de espacio considerable. Ya que mediante el uso de la virtualización evitamos la inversión en multitud de equipos físicos, esto supone un ahorro importante en mantenimiento, en consumo energético, espacio y procesos administrativos.

Por otro lado, mediante la virtualización y el balanceo dinámico podemos incrementar las tasas de prestación de servicios de un servidor del siguiente modo. Si disponemos de un servidor Web podemos asignar recursos adicionales al servidor, como por ejemplo memoria RAM y CPU en los picos de carga para evitar que el servidor se caiga y de este modo incrementar la tasa de eficiencia. Una vez finalizado el pico de carga podemos desviar los recursos aplicados al servidor Web a otra necesidad que tengamos. Por lo tanto, aparte de mejorar la tasa de servicio se pueden optimizar los recursos.

Si estamos usando una máquina virtual en un entorno de producción,

podemos ampliar los recursos de un sistema operativo o servidor de una forma muy sencilla, tan solo tenemos que acceder al Software de virtualización y asignar más recursos. Además, es fácil crear un entorno para realizar pruebas de todo tipo aislado del resto del sistema. Así, las máquinas virtuales y la virtualización permiten usar un solo servicio por servidor virtualizado de forma sencilla, de este modo aunque se caiga uno de los servidores virtualizados los otros seguirán funcionando.

En resumen, la virtualización permite ofrecer un servicio más rápido, sencillo a usuarios (académicos, estudiantes, clientes, etc.) y es un pilar que debe ser considerado en una escuela, universidad o compañía en su proceso de transformación o consolidación, permitiendo escalonar y ser creativos a la hora de atender las necesidades crecientes y cambiantes de los usuarios; y contar con servicios agregados, ágiles y adaptables a los constantes cambios de tecnología de Hardware y Software permitiendo escalar a la hiperconvergencia hacia la nube.

12.5.2 Desventajas

Entre las principales desventajas de virtualizar sistemas propietarios[114] como Windows (véase 11.1) -no así los sistemas libres como Debian GNU/Linux (véase 11.2)- es que se puede violar el sistema de licenciamiento (véase 11.5) del Software instalado en las máquinas virtuales, esto es especialmente importante cuando se usa en más de una máquina, pues la licencia usada para la instalación es violada cuando se tiene más de una copia de la máquina virtual o se ejecutan múltiples instancias de la máquina virtual.

En el caso de Windows XP Home, no se infringe la licencia mientras se cuente con número de licencias igual al máximo número de máquinas virtuales lanzadas simultáneamente. Para otras versiones del sistema operativo Windows como es Windows XP Profesional, la virtualización se maneja con licencias adicionales a la del sistema operativo original y se debe de contar con tantas licencias como el máximo número de máquinas virtuales lanzadas simultáneamente. Además, es necesario contar con el tipo de licencia adecuada para virtualizar a todos y cada uno de los paquetes de cómputo instalados en cada máquina virtual y en las instancias para el número de máquinas

[114] Según la Free Software Foundation (véase [12]), el «Software libre» se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, y estudiar el mismo, e incluso modificar el Software y distribuirlo modificado. Así, un Software que no es libre, es llamado «Software privativo o propietario».

virtuales lanzadas simultáneamente en uno o más equipos.

Para usar una máquina virtual en condiciones favorables, necesitamos un equipo de cómputo potente. Debemos tener en cuenta que si usamos dos sistemas operativos de forma simultánea estamos empleando hasta el doble de recursos. No obstante, cualquier equipo de cómputo doméstico de gama baja actual dispone de los recursos suficientes para usar una o más máquinas virtuales.

Los sistemas operativos y los programas se ejecutarán con mayor lentitud en las máquinas virtuales. Esto es debido a que las máquinas virtuales no pueden sacar un rendimiento ideal del Hardware que tenemos en nuestro equipo. Cuanto más potente sea nuestro equipo de cómputo menos se notará la pérdida de rendimiento.

Si tenemos un problema -de Hardware o Software- en el equipo de cómputo que aloja el sistema operativo anfitrión puede caerse el servicio en la totalidad de máquinas virtuales. Por lo tanto el equipo de cómputo que hace funcionar la máquina virtual es una parte crítica del proceso de virtualización.

A pesar de los inconvenientes que se citan en este apartado, bajo nuestro punto de vista, la virtualización y las máquinas virtuales proporcionan unas ventajas y una flexibilidad que compensan claramente los inconvenientes que acabamos de citar.

12.5.3 Consideraciones Técnicas y Legales de la Virtualización

Como se mostrará en la siguiente sección, virtualizar sistemas operativos -Linux, Unix, Windows entre otros- no representa ningún problema técnico, pero no es el caso en cuanto a las implicaciones legales de hacer la virtualización que involucra el almacenamiento, distribución y el número de veces que se ejecuta simultáneamente una máquina virtual en uno o múltiples equipos, ya que en general, la máquina virtual está contenida en un sólo archivo que facilita su distribución y almacenamiento, violando de esta forma la licencia de algunos sistemas operativos y/o programas instalados en el mismo.

En el caso de virtualizar cualquier sistema operativo libre como Debian GNU/Linux (véase 11.2), el tipo de licencia que tiene, permite y alienta su uso para cualquier fin que uno desee, por ello no hay ningún problema en virtualizarlo, no así el caso de hacerlo en sistemas operativos propietarios tipo Windows, la licencia (véase 11.1) restringe su uso a un sólo equipo de cómputo y en muchos casos prohíbe expresamente su virtualización. Además hay que

tomar en cuenta el resto del Software instalado en el sistema operativo, ya que estos también tienen sus propias restricciones legales a su uso y número de veces que se puede ejecutar simultáneamente un paquete dado.

Esto es especialmente importante cuando se usa en más de una máquina física, la misma máquina virtual, pues la licencia usada para la instalación es violada cuando se tiene más de una copia de la máquina virtual o se ejecutan múltiples instancias de la máquina virtual, esta violación de licencia es suficiente para ser sujeto a multas o incluso cárcel por dicho ilícito (véase 11.5).

Por otro lado, cada vez que se adquiere una licencia de uso de algún Software que no caduque -la cual implica un alto costo monetario-, esta pueda seguir siendo usada en una máquina virtual con una versión tal vez obsoleta del sistema operativo que la soporte, pero corriendo en un sistema huésped moderno y protegido en Hardware de última generación de forma lícita y con el consiguiente ahorro económico.

12.6 Máquinas Virtuales en la Educación, Ciencias e Ingeniería

Como hemos visto en las secciones anteriores, el uso de las máquinas virtuales es variado, flexible y permite ser usado en diversos ámbitos de la educación, del desarrollo y prueba de programas de cómputo y en general, en Ciencias e Ingeniería. Algunas de las utilidades y beneficios que podemos sacar de una máquina virtual son los siguientes:

- Para aprender a instalar, configurar y usar diversos sistemas operativos, además de poder probar diversas opciones de configuración en ellos. El proceso de instalación de la máquina virtual no requiere crear particiones adicionales en nuestro disco ni alterar la configuración de la máquina anfitriona y podemos trasladar la máquina virtual a uno o más equipos de cómputo que la soporte.

- Para usar un Software que no está disponible en nuestro sistema operativo habitual. Por ejemplo, si somos usuarios de Linux y queremos usar Photoshop, lo podemos hacer a través de una máquina virtual.

- En ocasiones tenemos que usar Software que únicamente se puede ejecutar en sistemas operativos obsoletos -Windows 98 por ejemplo-,

podemos crear una máquina virtual con dicho sistema y usar el Software de forma aislada sin preocuparnos de sus vulnerabilidades.

- Podemos experimentar en el sistema operativo que corre dentro de la máquina virtual haciendo cosas que no nos atreveríamos a realizar con nuestro sistema operativo habitual, como por ejemplo, instalar Software no seguro que consideramos sospechoso, etc.

- En muchos casos se quiere aprender a instalar, administrar y usar equipo al que no tenemos acceso como un equipo multiCore, con tarjeta CUDA instalada o un Cluster de múltiples nodos multiCore. Esto es posible hacer mediante el uso de máquinas virtuales en un equipo de gama media.

- Si se hace el adecuado aislamiento de una máquina virtual en la que se instale alguna versión de Windows, esta puede ser inmune a los virus y no requiere el uso de antivirus.

- En el caso de instituciones educativas de cualquier nivel académico, es común que en un mismo equipo de cómputo sea necesario ejecutar por un lado diferentes versiones de sistemas operativos -Linux, Windows XP, Windows 7, etc.- y por otro lado, en un sistema operativo, ejecutar diferentes versiones de un mismo paquete -generalmente no se puede tener instalada simultáneamente más de una versión- esto se logra con máquinas virtualizadas ad hoc coexistiendo en una misma máquina física.

- Podemos crear/simular una red de equipos de cómputo con tan solo un equipo de cómputo. Esta red de equipos de cómputo virtualizados la podemos usar con fines formativos y de este modo adquirir pericia sobre administración de redes.

- Si eres un desarrollador de Software puedes revisar si el programa que estas desarrollando funciona correctamente en varios sistemas operativos y/o navegadores de Web.

- Podemos usar las máquinas virtuales para hacer SandBox[115] con el fin

[115] Un sistema de aislamiento de procesos o entorno aislado, a menudo usando como medida de seguridad para ejecutar programas con seguridad y de manera separada del sistema anfitrión.

de ejecutar aplicaciones maliciosas o abrir correos sospechosos en un ambiente controlado y seguro.

- Para probar versiones Alfa, Beta y Release Candidate de ciertos programas y sistemas operativos.
- Para montar un servidor Web, un servidor VPN, un servidor de correo o cualquier otro tipo de servidor.
- Para probar multitud de programas en Windows y evitar que se ensucie el registro mediante las instalaciones y desinstalaciones de los programas
- Consolidar servidores, i.e. lo que ahora hacen varias máquinas, se pueden poner en un solo equipo físico dentro de varias máquinas virtuales independientes o interactuando entre ellas según se requiera.
- Mantenimiento y pruebas de aplicaciones sin necesidad de adaptar nuevas versiones del sistema operativo.
- Aumentar la disponibilidad al reducir tiempo de parada y mantenimiento. Ya que la máquina virtual está hecha, se pueden poner a trabajar una o más copias en un equipo o en múltiples máquinas físicas en cuestión de segundos, permitiendo la continuidad de un negocio o servicio y de recuperación ante desastres.
- Reducir costos de administración ya que se reducen y agilizan las políticas de respaldo y recuperación, además de optimizar los recursos disponibles permitiendo escalabilidad al crecer con contención de costos, mejorando la eficiencia energética al usar un menor número de equipos de cómputo.
- Permite incursionar en la estrategia de nube híbrida proactiva creando un conjunto de marcos de decisión en la nube y procesos para evaluar las oportunidades de computación en la nube en función de las necesidades y cargas de trabajo de los usuarios, por ejemplo el uso de supercómputo rentado.
- Establecer las habilidades, herramientas y procesos para un entorno dinámico e híbrido al asociarse los educadores y los especialistas en tecnologías de información para realizar un inventario de habilidades

y competencias, e identificar oportunidades de capacitación y áreas de vulnerabilidad potencial.

12.7 ¿Qué Necesito para Crear y Usar una Máquina Virtual?

Actualmente la virtualización de un sistema operativo se puede implementar por Software o por Hardware, lo único que precisamos para poder usar una máquina virtual es un equipo de cómputo e instalar y configurar el programa manejador de la máquina virtual. Cuanto más potente y actual sea el equipo de cómputo del que dispongamos, mejor experiencia obtendremos trabajando con sistemas operativos virtualizados.

Algunos de los puntos importantes para obtener un rendimiento óptimo del sistema operativo virtualizado son los siguientes:

- Preferentemente disponer de un procesador que disponga de capacidad de virtualización por Hardware (Intel VTx/AMD-V). Casi cualquier equipo de cómputo actual dispone de un procesador apto para virtualizar sistemas operativos por Hardware.
- Disponer de espacio suficiente en el disco duro[116], es preferible disponer de un disco de estado sólido (SSD) por sus velocidades de lectura-escritura.
- Necesitamos disponer de memoria RAM suficiente y adecuada[117]. Cuanta más memoria RAM y cuanto más rápida sea, mejores resultados de virtualización obtendremos.
- Sin duda el hecho de tener una buena tarjeta gráfica también ayudará a disponer de una mejor experiencia de virtualización.

Para empezar, debemos decidir qué manejador de máquinas virtuales usar, si trabajamos en Debian GNU/Linux, podemos usar QEMU/KVM y lo instalamos mediante:

[116] Una máquina virtual con Windows XP ocupa por lo menos 2 GB en disco y una con Windows 7 ocupa por lo menos 4 GB en disco.

[117] La cantidad de memoria RAM ideal dependerá del sistema operativo que queremos virtualizar y del número de sistemas operativos que queramos virtualizar de forma simultánea. Si tan solo queremos virtualizar un sistema operativo con 2 o 3 GB de RAM debería ser suficiente.

```
# apt install qemu-kvm qemu qemu-utils
```

QEMU/KVM soporta emulación de IA-32 (x86) PC, AMD64 PC, MIPS R4000, Sun's SPARC sun4m, Sun's SPARC sun4u, ARM development boards (Integrator/CP y Versatile/PB), SH4 SHIX board, PowerPC (PReP y Power Macintosh), y arquitecturas ETRAX CRIS.

Ejemplo 1 *Si hemos descargado la imagen ISO de algún sistema operativo, por ejemplo la de Knoppix*[118]*, la podemos usar mediante:*

```
$ kvm -m 1024 -cdrom KNOPPIX_ V8.2-2018-05-10-EN.iso
```

Aquí se usa la arquitectura por omisión y memoria de 1024 MB.

Ejemplo 2 *Instalación y uso de una máquina virtual para Debian GNU/Linux estable a partir del archivo ISO*[119]*, para ello, primero necesitamos:*

Generar el disco virtual que la contendrá, por ejemplo de 10 GB con el nombre debianStable.img mediante:

```
$ qemu-img create -f qcow2 debianStable.img 10G
```

Después, instalar la imagen de Debian estable en el disco virtual genera-do en el paso anterior, solicitando a KVM que una vez terminada la instalación no haga el reinicio de la máquina virtual, esto mediante:

```
$ kvm -no-reboot -boot d -cdrom debian-802-i386-netinst.iso \
-hda debianStable.img -m 400
```

Ahora podemos usar la máquina virtual mediante:

```
$ kvm -hda debianStable.img -m 800
```

Ejemplo 3 *Instalación y uso de una máquina virtual para Windows XP, en este caso necesitamos:*

Crear el disco virtual, por ejemplo de 10 GB mediante:

```
$ qemu-img create -f qcow2 WindowsXP.img 10G
```

Hacer la instalación básica a partir del ISO, mediante:

```
$ kvm -no-reboot -boot d -hda WindowsXP.img -m 400 \
-localtime -cdrom es_ winxp_ pro_ with_ sp2.iso
```

Y concluir la instalación mediante:

```
$ kvm -no-reboot -boot c -hda WindowsXP.img -m 400 \
```

[118] Knoppix es una versión Live ampliamente conocida y completa de GNU/LINUX, se puede descargar de: https://www.knopper.net/knoppix/

[119] Diversas imágenes ISO del proyecto Linux Debian se pueden descargar de: https://www.debian.org/CD/

-localtime -cdrom es_winxp_pro_with_sp2.iso
Ahora podemos usar la máquina virtual mediante:
$ kvm -boot c -hda WindowsXP.img -m 400 -localtime

12.8 ¿Cómo Funciona una Máquina Virtual?

Explicar el funcionamiento a detalle de una máquina virtual es engorroso y está fuera del alcance del propósito de este texto. No obstante a grandes rasgos podemos decir que una máquina virtual es un Software que mediante una capa de virtualización[120] se comunica con el Hardware que tenemos disponible en nuestro equipo de cómputo consiguiendo de este modo emular la totalidad de componentes de un equipo de cómputo real. De este modo la máquina virtual será capaz de emular un disco duro, una memoria RAM, una tarjeta de red, un procesador, etc.

Una vez que sabemos esto, cuando abrimos una máquina virtual, como por ejemplo Virtualbox (véase [18]), nos encontramos con un entorno gráfico (en el caso de usar QEMU/KVM se usa la línea de comandos para crear y usar las máquinas virtuales, pero también se cuentan con entornos gráficos que usan la línea de comandos internamente) que nos permitirá configurar y asignar recursos a cada uno de los componentes físicos que emula la máquina virtual. En prácticamente la totalidad de máquinas virtuales debemos definir detalles del siguiente tipo:

- Tipo de procesador a usar
- Espacio que queramos asignar al disco duro.
- Memoria RAM que queremos asignar a la máquina virtual.
- La memoria de nuestra tarjeta gráfica.
- La configuración de red.
- etc.

[120] La capa de virtualización es un sistema de archivos propietario y una capa de abstracción de servicio del Kernel que garantiza el aislamiento y seguridad de los recursos entre distintos contenedores. La capa de virtualización hace que cada uno de los contenedores aparezca como servidor autónomo. Finalmente, el contenedor aloja la aplicación o carga de trabajo.

Una vez configurados estos parámetros habremos creado una máquina virtual para instalar un sistema operativo, de este modo tan solo tendremos que abrir la máquina virtual que se acaba de crear e instalar el sistema operativo tal y como si se tratará de un equipo de cómputo real.

12.9 Aplicaciones y Paquetes Disponibles

A continuación mencionaremos algunas de las aplicaciones más conocidas y universalmente disponibles y/o usadas en los Sistemas Operativos GNU Linux/BSD, tanto en el ámbito personal, es decir, distribuciones usadas para fines particulares (hogar), como en el ámbito profesional, es decir, en el área de servidores de organizaciones y empresas.

Es importante destacar que, en este listado no se incluirán aquellas tecnologías de virtualización que vienen como una solución integrada, todo en uno o llave en mano, tales como *Promox*.

VirtualBox Software desarrollado por Oracle multiplataforma, capaz de virtualizar prácticamente la totalidad de sistemas operativos con arquitectura x86/amd64. La base de este Software dispone de una licencia GPL2, mientras que el Pack de extensiones que añaden funcionalidades están bajo licencia privativa. Virtualbox es gratuito para un uso no comercial.

Es un Hipervisor de Tipo 2 multiplataforma, es decir, solo debe y puede ser ejecutado (instalado) en cualquier Host (Ordenador) con alguna de las versiones vigentes o antiguas de Sistemas Operativos Windows, Linux, Macintosh, Solaris, OpenSolaris, OS/2 y OpenBSD.

Posee un continuo y progresivo ciclo de desarrollo con lanzamientos frecuentes, que la convierten en una excelente alternativa a otras soluciones parecidas, pero con una muy apreciable cantidad de características y funciones, sistemas operativos invitados compatibles y plataformas en las que se puede ejecutar.

En la mayoría de las distribuciones GNU Linux/BSD se encuentra dicha aplicación incluida en los repositorios, por lo que, con la siguiente orden de comando suele instalarse en todas ellas:

```
# apt install virtualbox
```

Vale destacar para VirtualBox que, al usar esta aplicación siempre es ideal la instalación de las «Guest Additions» y el «Extension Pack». Por ende,

para esto y otras formas de instalación lo ideal es visitar el enlace oficial de VirtualBox.

Vmware Workstation Player Software privativo multiplataforma desarrollado por EMC Corporation y que es utilizado ampliamente en el entorno profesional en las áreas del Cloud Computing entre muchas otras. Al igual que Virtualbox, esta máquina virtual nos permite virtualizar infinidad de sistemas operativos. Vmware dispone de muchas soluciones de virtualización y prácticamente todas son de pago, no obstante Vmware Workstation Player es totalmente gratuita para un uso no comercial.

Parallels aunque se trata de una máquina virtual multiplataforma, acostumbra a ser usado por los usuarios del sistema operativo OS X de Apple que desean virtualizar el sistema operativo Windows. Esta máquina virtual es de pago y únicamente puede virtualizar los sistemas operativos Windows y Mac OS. Quien quiera probar Parallels lo puede hacer descargando la versión de prueba.

Windows Virtual PC Software gratuito y privativo propiedad de Microsoft que se puede usar tanto en Windows como en Mac OS. Virtual PC está destinado únicamente a virtualizar sistemas operativos Windows.

Virtualización: GNOME Boxes es una aplicación nativa del entorno de Escritorio GNOME, que se utiliza para acceder a sistemas remotos o virtuales. Boxes o Cajas, utiliza las tecnologías de virtualización de *QEMU*, *KVM* y *Libvirt*.

Además, requiere que la CPU sea compatible con algún tipo de virtualización asistida por Hardware (Intel VT-x o AMD-V, por ejemplo); por lo tanto, GNOME Boxes no funciona en las CPUs con procesador Intel Pentium/Celeron, ya que, carecen de esta característica.

En la mayoría de las distribuciones GNU Linux/BSD se encuentra dicha aplicación incluida en los repositorios, por lo que, con la siguiente orden de comando suele instalarse en todas ellas:

```
# apt install gnome-boxes
```

Vale destacar para GNOME Boxes que, es una herramienta muy sencilla dirigida a usuarios novatos, permite descargar desde la aplicación diversas

imágenes y no incorpora demasiadas opciones de configuración que suelen ser muy conocidas y usadas en otras, tales como VirtualBox.

Virt-Manager es una interfaz de usuario de escritorio para la administración de un Gestor de Máquinas Virtuales a través de *Libvirt*. Está dirigida principalmente a las máquinas virtuales gestionadas por *KVM*, pero también maneja las gestionadas por *Xen* y *LXC*.

Virt-Manager presenta una vista resumida de los dominios en ejecución, su rendimiento en vivo y estadísticas de utilización de recursos. Los asistentes permiten la creación de nuevos dominios, y la configuración y ajuste de la asignación de recursos de un dominio y el Hardware virtual. Un visor de cliente *VNC* y *SPICE* integrado presenta una consola gráfica completa para el dominio invitado.

En la mayoría de las distribuciones GNU Linux/BSD se encuentra dicha aplicación incluida en los repositorios, por lo que, con la siguiente orden de comando suele instalarse en todas ellas:

```
# apt install virt-manager
```

Vale destacar para Virt-Manager que, es también es una herramienta sencilla, aunque mucho más completa que GNOME Boxes, por lo que se puede considerar para usuarios medios o avanzados de primer nivel, dado que, fácilmente es capaz de permitir la gestión de todo el ciclo de vida de las máquinas virtuales existentes.

QEMU / KVM es un emulador y virtualizador de máquinas genérico y de código abierto, capaz de ejecutar sistemas operativos y programas hechos para una máquina en una máquina diferente con muy buen rendimiento, y capaz de lograr un rendimiento casi nativo ejecutando el código del huésped directamente en la CPU del Host.

KVM es una solución de virtualización completa para Linux en Hardware x86 que contiene extensiones de virtualización (Intel VT o AMD-V) que consiste en un módulo de Kernel cargable, que proporciona la infraestructura de virtualización del núcleo y un módulo específico del procesador. Y actualmente funciona inmerso dentro de QEMU.

En la mayoría de las distribuciones GNU Linux/BSD se encuentra dicha aplicación incluida en los repositorios, por lo que, con la siguiente orden de comando suele instalarse en todas ellas:

```
# apt install qemu-kvm
```

además, en caso necesario podemos hacer uso de una interfaz gráfica para trabajar con QEMU/KVM, tenemos varias opciones, algunas de ellas son:

```
# apt install qemu-system-gui
# apt install aqemu
# apt install qemuctl
# apt install virt-manager
# apt install gnome-boxes
```

Vale destacar que QEMU/KVM es también es una herramienta muy completa, ya que no solo emula (x86, x86-AMD64, MIPS, Arm, PowerPC, SPARC, etc.) sino que virtualiza, a diferencias de otros iguales de avanzadas como WMWare, que solo permite virtualizar. Para conocer las opciones de emulación usamos:

```
$ apt search qemu-system-
```

Cockpit es una interfase Web Open Source que permite manejar máquinas virtuales de KVM que provee acceso a sistemas Linux permitiendo la administración, manejo y monitoreo a través de una interfaz gráfica intuitiva, para usarlo hay que instalar primero KVM y luego hacer:

```
# apt install cockpit cockpit-machines
```

Librerías y Paquetes relacionados Estos últimos 3 paquetes mencionados suelen instalar otros conexos (relacionados) como dependencias, por lo que, en caso de ser necesario, pueden instalar los mismos, junto a sus dependencias y otros paquetes útiles necesarios, como:

```
gnome-boxes virt-manager virt-goodies virt-sandbox virt-top
virt-viewer virtinst libvirt-clients libvirt-daemon libvirt-daemon-
system qemu qemu-kvm qemu-utils qemu-system qemu-system-
gui qemu-block-extra freerdp2-x11 bridge-utils ovirt-guest-agent
systemd-container
```

Otros en caso de querer instalar otras tecnologías de virtualización disponibles sobre Linux/BSD se puede optar por:

Xen instalándolo con la orden de comando siguiente:

```
# apt install xen-system-amd64 xen-utils-4.11 xen-tools
```

LXC instalándolo con la orden de comando siguiente:

```
# apt install lxc
```

Docker instalándolo con la orden de comando siguiente:

```
# apt install docker-ce docker-ce-cli containerd.io
```

Diferencias entre KVM y QEMU Cuando comenzamos en el mundo de la virtualización, la opción más recurrente para comenzar es KVM. Después nos damos cuenta de que se comienza a usar también otro componente muy a menudo, QEMU y siempre hay muchas preguntas en torno a cómo funciona KVM y QEMU o cual es la diferencia entre ellos.

Sobre KVM es un Software de código abierto y significa Kernel Virtual Machine (Máquina Virtual basada en el Kernel) es una solución de virtua-lización para Linux en hardware x86 que contiene extensiones de virtualización (Intel VT o AMD-V). KVM forma parte del Kernel de Linux desde la versión 2.6.20. Específicamente, con KVM podemos convertir a Linux en un hipervisor para que nuestro Host ejecute entornos virtuales, es decir, máquinas virtuales. Cada máquina virtual se implementa como un proceso regular de Linux

KVM ha jugado un papel clave en el entorno de virtualización de código abierto basado en Linux. De hecho, KVM es el único hipervisor para todos los productos de virtualización de Red Hat, tanto para RHOSP - Red Hat Openstack Platform, como para Red Hat Virtualization o abreviado, RHV.

KVM en general es 2 cosas, un módulo del Kernel pero también KVM es es un Fork del ejecutable de QEMU (más adelante hablaremos de eso). Entonces como mencionamos, KVM es un módulo Kernel que permite el uso de tecnologías de extensiones de virtualización Intel o AMD. En pocas palabras, estas extensiones permiten que múltiples sistemas operativos compartan una CPU física sin interferir entre ellos. Por otro lado, no resuelven compartir todos los dispositivos de Hardware, para esto KVM requiere una lógica extra y aquí es dónde comenzamos a hablar de QEMU.

Sobre QEMU es un emulador de procesadores basado en la traducción dinámica de binarios, es decir, realiza la conversión del código binario de la arquitectura fuente o Host, en código entendible por la arquitectura huésped o la máquina virtual.

El resultado de usar QEMU es poder ejecutar el código original como si se estuviera ejecutando en la máquina emulada. Por ejemplo, se podría ejecutar código escrito para el procesador ARM en su máquina basada en Intel.

QEMU es capaz de emular varias plataformas de Hardware diferentes, incluida la x86, plataformas PowerPC, sistemas basados en ARM y también sistemas SUN SPARC. Además del Hardware básico de estos sistemas, QEMU también proporciona emulación de varios módulos adicionales, como tarjetas gráficas, tarjetas de sonido, dispositivos de red, dispositivos de almacenamiento y controladores, dispositivos serie/paralelo/USB y dispositivos de memoria. Esto significa que en muchos casos las computadoras pueden ser completa y totalmente emuladas y utilizadas para ejecutar su Software original.

¿Cómo trabajan juntos? en el Hardware real, el sistema operativo traduce las instrucciones de los programas para que sean ejecutadas por el CPU físico. En una máquina virtual es lo mismo, pero la diferencia es que el CPU está virtualizado por el hipervisor y el hipervisor tiene que traducir las instrucciones del CPU virtual y convertirlo en instrucciones para el CPU físico. Esta traducción tiene una gran sobrecarga de rendimiento.

Para minimizar esta sobrecarga, los procesadores admiten extensiones de virtualización. Intel soporta una tecnología llamada VT-X y el equivalente AMD es AMD-V. Con el uso de estos, una rebanada de CPU físico se puede asignar directamente al CPU virtual. Así que las instrucciones de la CPU virtual se pueden ejecutar directamente en la rebanada del CPU físico. Evitando así la traducción que tendría que hacer el hipervisor.

KVM es el módulo del Kernel de Linux que permite esta asignación de CPU físico para CPU virtual. Esta asignación proporciona la aceleración de Hardware para la máquina virtual y aumenta su rendimiento. De hecho QEMU utiliza esta aceleración cuando el tipo de virtualización es elegido como KVM.

Los desarrolladores de KVM aprovecharon la arquitectura QEMU y básicamente crearon un nuevo modelo de CPU en QEMU. Este nuevo tipo de modelo tiene una lógica específica de KVM. Así las llamadas al sistema que

se harían de forma nativa pasan por del módulo KVM para que la ejecución se ejecute de forma nativa en la CPU, mientras que QEMU se utiliza para proporcionar el resto funcionalidad (emular los dispositivos).

Al trabajar juntos, KVM accede directamente al CPU físico y a la memoria, a su vez QEMU emula los recursos de Hardware, como el disco duro, video, USB, etc. Hoy, cuando las personas se refieren al hipervisor KVM, en realidad se refieren a la combinación QEMU/KVM.

KVM necesita QEMU (emulador) para la funcionalidad completa como hipervisor. QEMU es autosuficiente y KVM es realmente un módulo del Kernel de Linux para la explotación de extensiones VT que actúa como controlador de las capacidades de CPU físicas.

Así puedes notar entonces que QEMU necesita a KVM para aumentar su rendimiento... Por otro, lado KVM por sí solo no puede proporcionar la solución de virtualización completa, necesita de QEMU.

12.10 Acceso a Datos Desde una Máquina Virtual

Para acceder a los datos almacenados en máquinas virtuales, disponemos de las siguientes opciones:

a) Mediante el uso de algún navegador Web, se puede acceder a su cuenta de correo electrónico y al almacenamiento en la nube como *Google Drive, Dropbox, HubiC, pCloud, MediaFire, FlipDrive, Mega*, entre otros.

b) En el sistema operativo Linux, se puede acceder a cualquier servidor de internet mediante los protocolos *SSH*, *SAMBA* o montar un sistema de archivos mediante *NFS* o *SSHFS*, entre otros.

c) En cualquier sistema operativo podemos usar algún navegador gráfico de *FTP, FTPS o SFTP* como *FileZilla, WinSCP, PSCP, PSFTP, FireFTP, CoreFTP*, entre muchos otros, para transportar archivos y carpetas.

d) En las máquinas virtuales de Windows usamos el protocolo *SAMBA*, para tener acceso a este, hay que conectarse a una unidad de red dentro del explorador de archivos de Windows.

e) En Linux, por ejemplo con *PCManFM, Dolphin, Nautilus, Thunar, Konqueror*, entre otros, podemos acceder a una máquina que tenga un servidor de la siguiente forma:

1) Para acceder a un servidor *SAMBA*, escribir la ruta de archivos en el manejador de archivos:

$ smb://estud@192.168.13.230/estud/

2) Para acceder a un servidor *SSH*, escribir la ruta de archivos en el manejador de archivos:

$ sftp://usuario@192.168.13.230/home/usuario/

En línea de comandos, podemos:

3) Montar con *SSHFS* un directorio de otra máquina con servidor *SSH*:

$ sshfs usuario@192.168.13.230:/home/usuario/ /home/algun/lugar

4) Montar con mount un directorio de otra máquina con servidor *NFS*:

mount 10.0.2.2:/directorio ./punto_montaje

5) Usar *SCP* y *SFTP* de *SSH* para transferir archivos, para copiar un archivo, usamos:

$ scp archivo.dat usuario@192.168.13.230:~/Datos/

para copiar un subdirectorio, usamos:

$ scp -r Directorio usuario@192.168.13.230:.

para copiar un archivo de una máquina remota a nuestra máquina, usamos:

$ scp usuario@192.168.13.230:/home/usuario/archivo .

6) Montar con CURLFTPFS un directorio de otra máquina con servidor *FTP*:

curlftpfs -o allow_other usuario:password@192.168.13.230:puerto /home/algun/lugar

12.11 Desde la Nube

Existen diferentes servicios Web[121] que permiten instalar, configurar y usar cientos de sistemas operativos Linux y Unix -máquinas virtuales usando servicios Web en Debian GNU/Linux y QEMU- desde el navegador, esto en

[121] Cuando se trabaja desde la Web es recomendable usar el modo Privado o Incógnito para no guardar el historial de navegación, información introducida en los formularios y borrar al cerrar el navegador los datos de los sitios visitados. Pero recuerda que los sitios Web que visitamos sí guardan información de nuestra visita, nuestro proveedor de internet también guarda constancia de nuestra visita y si descargamos algo, esto no se borra al igual que el historial de descargas, además de las marcas de páginas o favoritos se conservarán al cerrar el navegador.

aras de que los usuarios que cuenten con algún sistema de acceso a red y un navegador puedan usar, configurar e instalar algún sistema operativo y su respectiva paquetería sin hacer instalación alguna en su equipo de cómputo, tableta o teléfono celular[122].

Una muestra de estos proyectos son: Distrotest (https://distrotest.net) y JSLinux (https://bellard.org/jslinux).

Algunas versiones listas para usar son:

4mLinux, AbsoluteLinux, Academix, AlpineLinux, Antergos, antiX Linux, Aptosid, ArchBang, ArchLabs, ArchLinux, Archman, ArchStrike, ArcoLinux, ArtixLinux, AryaLinux, AV Linux, BackBoxLinux, BigLinux, Bio-Linux, BlackArch, BlackLab, BlackPantherOS, BlackSlash, blag, BlankOn, Bluestar, Bodhi, BunsenLabs, ByzantineOS, Caine, Calculate Linux Desktop, CentOS, Chakra, ChaletOS, ClearOS, Clonezilla, ConnochaetOS, Cucumber, Damn Small Linux, Damn Small Linux Not, Debian, DebianEdu, deepin, DEFT, Devil-Linux, Devuan, DragonFly BSD, Dragora, DuZeru, Dyne:bolic, Edubuntu, elementaryOS, Elive Linux, Emmabuntüs, Emmi OS, Endless OS, EnsoOS, Exe GNU/Linux, ExTiX, Fatdog64, Fedora Atomic, Fedora Server, Fedora Workstation, FerenOS, FreeBSD, FreeDOS, Frugalware, G4L, GeckoLinux, Gentoo, GNewSense, GoboLinux, Gparted, GreenieLinux, GRML, GuixSD, Haiku, Heads, Kali Linux, Kanotix, KaOS, Knoppix, Kodachi, KolibriOS, Korora, Kubuntu, Kwort, Linux Lite, Linux Mint, LiveRaizo, LMDE, Lubuntu, LXLE OS, Macpup, Mageia, MakuluLinux, Manjaro, Matriux, MauiLinux, MenuetOS, MinerOS, MiniNo, Modicia, Musix, MX Linux, Nas4Free, Neptune, NetBSD, Netrunner, NixOs, NST, NuTyX, OpenIndiana, OpenMandriva, openSUSE, OracleLinux, OSGeo live, OviOS, Parabola CLI, Parabola LXDE, Pardus, Parrot Home, Parrot Security, Parrot Studio, Parsix, PCLinuxOS, PeachOSI, Pentoo, Peppermint, PeppermintOS, Pinguy, PinguyOS, plopLinux, PointLinux, Pop!_OS, PORTEUS, Puppy Linux, PureOS, Q4OS, QubesOS, Quirky, Raspberry Pi Desktop, ReactOS, Redcore, Rescatux, RevengeOS, RoboLinux, Rockstor, ROSA FRESH, Runtu, Sabayon, SalentOS, Salix, ScientificLinux, Siduction, Slackware, Slax, SliTaz, Solus, SolydK, SolydX, SparkyLinux, Springdale, StressLinux, SubgraphOS, SwagArch, Tails, Tanglu, Tiny Core, Trisquel, TrueOS, TurnKey Linux, Ubuntu, Ubuntu Budgie, Ubuntu Studio, UbuntuKylin, Uruk, VectorLinux, VineLinux, VoidLinux, Voyager, VyOS, WattOs, Xubuntu, Zentyal, Zenwalk, Zevenet, Zorin OS

Usar Linux en Formato Live Linux es uno de los sistemas operativos pioneros en ejecutar de forma autónoma o sin instalar en la computadora, existen diferentes distribuciones Live -descargables para formato CD, DVD, USB[123]- de sistemas operativos y múltiples aplicaciones almacenados en un medio extraíble, que pueden ejecutarse directamente en una computadora,

[122] Estos servicios son conocidos como computación en la nube (Cloud Computing).

[123] Para generar un dispositivo USB con la imagen contenida en un archivo ISO podemos usar el Software ETCHER, descargable para Linux, Windows y Mac OS desde https://etcher.io/.

estos se descargan de la Web generalmente en formato ISO[124], una de las listas más completas de versiones Live está en:

https://livecdlist.com

En el caso de tener un archivo ISO de algún sistema operativo (por ejemplo ubuntu-11.10-desktop-i386.iso) y se quiere ejecutar su contenido desde una máquina virtual con QEMU/KVM sólo es necesario usar:

```
$ kvm -m 512 -cdrom ubuntu-11.10-desktop-i386.iso
```

en este ejemplo usamos en KVM la arquitectura por omisión y memoria de 512 MB (-m 512).

Knoppix es una versión Live ampliamente conocida y completa, esta se puede descargar de:

https://www.knopper.net/knoppix/

y usar mediante:

```
$ kvm -m 1024 -cdrom KNOPPIX_V8.2-2018-05-10-EN.iso
```

aquí se usa la arquitectura por omisión y memoria de 1024 MB.

Descarga de Máquinas Virtuales de Sistemas Operativos Existen diversos proyectos que permiten descargar decenas de máquinas virtuales listas para ser usadas, para los proyectos VirtualBox y VMWare (y por ende para KVM/QEMU), estas se pueden descargar de múltiples ligas, algunas de ellas son:

https://www.osboxes.org
https://www.virtualbox.org

Si desargamos y descomprimimos el archivo lubuntu1210.7z, esto dejará la imagen de VirtualBox de LUBUNTU cuyo nombre es lubuntu1210.vdi. Entonces esta imagen la usaremos directamente en KVM/QEMU, mediante:

```
$ kvm -m 2000 -hda lubuntu1210.vdi
```

Nota: esta imagen usa como usuario y clave de acceso: lubuntu/lubuntu

[124] Una imagen ISO es un archivo informático donde se almacena una copia exacta de un sistema de archivos y de esta se puede generar una imagen para CDROM, DVD o USB.

13 Apéndice C: Escritorios Remotos y Virtuales

Con el propósito de que cualquier usuario que cuente con un dispositivo de cómputo[125] con red[126] puedan usar, configurar o instalar aplicaciones en los ambientes computacionales que se tienen instalados en otros equipos de forma remota, se crearon los escritorios remotos y los escritorios virtuales. Estos permiten visualizar la salida gráfica -de un sistema operativo en múltiples equipos o diversos sistemas operativos en un mismo equipo- por medio de internet (aún si la velocidad de conexión es baja).

Los casos de uso son muchos y se centran muy especialmente en los ámbitos de la asistencia remota[127] y del teletrabajo.

Escritorio Remoto Esta es una de las muchas aplicaciones que permiten acceder a un equipo de cómputo remoto mediante internet y controlarlo como si estuviéramos delante de él -más o menos-. Con estas aplicaciones, nos ahorramos tener que desplazarnos hasta donde está el equipo de cómputo al que queremos conectarnos, y así podemos por ejemplo ofrecer asistencia remota desde nuestro equipo de cómputo o usar los programas que se tienen instalados en un equipo remoto.

Algunas opciones de escritorios remotos[128] son:

- Chrome Escritorio Remoto (de descarga y uso gratuito), donde instalamos el servidor de escritorio remoto a través del navegador Chrome (o Chromium) en el equipo de cómputo a controlar y mediante el navegador Chrome en el otro equipo, se puede acceder remotamente cuando se necesita desde cualquier lugar con internet.

[125] Puede ser computadora personal , tableta, teléfono inteligente, Chromebook corriendo algún sistema operativo como Windows, Linux, MacOS, Android, Raspberry PI, IOS, Chrome, Solaris, HP-UX, AIX, etc.

[126] ¡Claro desde casa!, sin dirección IP pública fija homologada.

[127] Si algo no le funciona a alguien, estos servicios remotos nos permiten "meternos" en su equipo de cómputo y solucionarlo, incluso explicando mientras se está haciendo, porque se toma el control del teclado, ratón y pantalla, pero el usuario sigue teniendo control si quiere retomarlo y puede ver todo lo que hacemos en el escritorio remoto.

[128] Otras opciones son: Apple Remote Desktop, TeamViewer, SupRemo, Ammyy Admin, Iperius Remote, AnyDesk, VNC Connect, etc.

- "Asistencia rápida" (o Quick Assist) de Windows 10 es una utilidad del sistema operativo que permite a dos personas compartir un equipo mediante conexión remota, pero sin necesidad de descargar ni instalar nada adicional.

Escritorio Virtual Es el acceso a un equipo de cómputo virtual en la nube, cuyo poder de procesamiento no se encuentra en un equipo de cómputo físico, sino en servidores ubicados en un centro de datos.

El usuario inicia sesión con sus credenciales y accede a un escritorio con las aplicaciones y programas instalados como si estuviera sentado frente a ese equipo de cómputo virtual.

¿Cuáles son las ventajas? los escritorios virtuales[129] tienen muchas ventajas para las organizaciones que necesitan entregar acceso a un equipo de cómputo con un conjunto establecido de aplicaciones. Se reducen los costos administrativos y mantenimiento de licencias. También facilita la solución de problemas de usuario y reduce problemas de seguridad.

Otras ventajas de esta tecnología:

1.- Administración centralizada de aplicaciones

2.- Se puede acceder desde dispositivos móviles, como teléfonos o tabletas.

3.- Facilita la aplicación de políticas organizacionales.

4.- Acelera la habilitación de nuevos puntos de trabajo.

Desde hace años existen ejemplos de estas tecnologías: "Windows Virtual Desktop" el escritorio virtual de Windows 10 sobre Microsoft Azure y recientemente con: "Cloud PC" para ofrecer "Desktop as a Service" de la división "Cloud Managed Desktops" de Microsoft.

Tipos de Servicios en la Nube Hay tres tipos principales de servicios en la nube: Software como servicio (SaaS) , Plataforma como servicio (PaaS) e Infraestructura como servicio (IaaS). No existe un enfoque único para la nube. Lo ideal es encontrar la solución adecuada que respalde los requisitos de un grupo de usuarios o empresa.

[129] Ejemplo de estos productos son: VMware Horizon, Citrix Virtual Apps and Desktops, Oracle Secure Global Desktop, HP Workspace, Amazon WorkSpaces, Parrallels Remote Application Server, Microsoft Windows Virtual Desktop, etc.

SaaS y sus beneficios el Software como servicio (SaaS) es un modelo de entrega de Software en el que las aplicaciones del cliente están alojadas en las instalaciones del proveedor de la nube. El cliente accede a sus aplicaciones a través de internet. En lugar de pagar y mantener su propia infraestructura informática, el cliente aprovecha la suscripción al servicio de pago por uso.

Muchas empresas consideran que SaaS es la solución ideal porque les permite ponerse en marcha rápidamente con la tecnología más innovadora disponible. Las actualizaciones automáticas reducen la carga sobre los recursos internos. Los clientes pueden ampliar la escala de sus servicios para afrontar las cargas de trabajo fluctuantes y agregar más servicios o funciones a medida que van creciendo. Una suite de nube moderna proporciona un Software completo para cada necesidad empresarial, como la experiencia del cliente, la adquisición de ERP, la administración de la cartera de proyectos ERP, la cadena de suministro y la planificación empresarial.

PaaS y sus beneficios la plataforma como servicio (PaaS) brinda a los clientes la ventaja de acceder a las herramientas de desarrollador que necesitan para crear y administrar aplicaciones móviles y Web sin necesidad de invertir ni mantener la infraestructura subyacente. El proveedor aloja la infraestructura y los componentes de Middleware y el cliente accede a esos servicios a través de un navegador Web.

Para ayudar a la productividad, el proveedor de servicio PaaS ofrece componentes de programación listos para usar que permiten a los desarrolladores agregar nuevas capacidades a sus aplicaciones, incluidas tecnologías innovadoras tales como inteligencia artificial (IA), Chatbots, Blockchain e internet de las cosas (IoT). También incluye soluciones para analistas, usuarios finales y administradores profesionales de técnologías de la información (TI), incluidos análisis de Big Data, administración de contenido, administración de base de datos, administración de sistemas y seguridad.

IaaS y sus beneficios la infraestructura como servicio (IaaS) permite a los clientes acceder a servicios de infraestructura a pedido a través de internet. La ventaja clave es que el proveedor de la nube aloja los componentes de la infraestructura que proporcionan capacidad de cómputo, almacenamiento y red para que los suscriptores puedan ejecutar sus cargas de trabajo en la nube. El suscriptor de la nube generalmente es responsable de instalar, configurar, asegurar y mantener cualquier Software que se encuentre dentro

de la infraestructura basada en la nube, como la base de datos, el Middleware y el Software de aplicación.

Beneficios del cómputo en la nube hay varias tendencias que impulsan a los usuarios y las empresas de todas las industrias a migrar hacia la nube. Para la mayoría de las organizaciones, la forma actual de hacer negocios podría no ofrecer la agilidad para crecer ni proporcionar la plataforma o la flexibilidad necesarias para competir. La explosión de datos creada por un número cada vez mayor de empresas digitales está llevando el costo y la complejidad del almacenamiento del centro de datos a nuevos niveles. Eso requiere nuevas habilidades y herramientas de análisis por parte del departamento de TI.

Las soluciones que ofrece la nube moderna ayudan a los usuarios y las empresas a enfrentar los desafíos de la era digital. En lugar de administrar su propia TI, la nube permite que las organizaciones respondan rápidamente a un panorama comercial más acelerado y complejo.

De qué manera la nube puede fomentar la innovación los clientes de la nube tienen automáticamente las últimas innovaciones y tecnologías emergentes integradas en sus sistemas de TI. El proveedor de la nube asume la responsabilidad de desarrollar nuevas capacidades y características. Los clientes que están en la nube obtienen esa ventaja estratégica.

Lo importante es la velocidad de la innovación. Los clientes de un proveedor pueden aprovechar una arquitectura de cómputo de nube moderna para innovar más rápido, aumentar la productividad y reducir los costos. Las capacidades integradas en la nube de múltiples proveedores (SaaS, PaaS e IaaS) proporcionan a las empresas la capacidad de pasar de las operaciones a la innovación. Las empresas pueden ofrecer nuevas aplicaciones y servicios, incluido el uso de tecnologías innovadoras como la inteligencia artificial (IA), Chatbots, Blockchain e internet de las cosas (IoT). Las empresas pueden aprovechar la abundancia de datos para obtener información predictiva de sus negocios y, en última instancia, obtener mejores resultados para sus clientes.

Confianza y seguridad Mudarse a la nube elimina los dolores de cabeza y los costos de mantener la seguridad de TI. Un proveedor de nube experimentado invierte continuamente en la última tecnología de seguridad,

no solo para responder a posibles amenazas, sino también para permitir que los clientes cumplan mejor los requisitos de las reglamentaciones aplicables. Destacando que, la gran mayoría de estos servicios corren bajo alguna variante del sistema operativo Linux y dentro de él, se corren máquinas virtuales de diversos sistemas operativos según lo requiera el usuario.

13.1 Escritorio Remoto

Por un lado, si eres una de esas personas a los que colegas, amigos o familiares constantemente le piden ayuda para "arreglar su equipo de cómputo" porque creen que eres el que más sabe de tecnología, o por el otro estas desesperado porque necesitas ayuda en tu equipo de cómputo, entonces necesitas conocer la maravillosa herramienta de escritorio remoto.

Los programas "Chrome Escritorio Remoto" y "Asistencia Rápida de Windows" son dos de las muchas aplicaciones[130] que permiten acceder a un escritorio remoto y controlarlo remotamente como si estuviéramos delante de él -más o menos- cuando se necesita, desde cualquier lugar con internet.

En el caso de "Chrome Escritorio Remoto" es un servicio multiplataforma que solo requiere tener instalado el navegador Chrome -o sus derivados- para permitir el acceso sobre internet al equipo que se requiera. En el caso de "Asistencia Rápida" de Windows todo está listo para ser usado, pues es un paquete que viene integrado al sistema operativo Windows.

A continuación describiremos cómo usar dichos escritorios remotos.

13.1.1 Escritorio Remoto de Chrome

Es posible utilizar un equipo de cómputo o un dispositivo móvil para acceder a las aplicaciones y los archivos guardados en otro equipo de cómputo a través

[130] Si requiere de información adicional de algunos clientes de el escritorio remoto (para Windows, Linux, MacOS, Android, Raspberry PI, IOS, Chrome, Solaris, HP-UX, AIX) puede consultarlos en:
https://www.nobbot.com/pantallas/escritorio-remoto-en-chrome-como-instalarlo/
https://www.xataka.com/basics/escritorio-remoto-chrome-como-configurarlo-para-manejar-tu-ordenador-a-distancia
https://business.tutsplus.com/es/articles/best-remote-access-desktop-software–cms-31917
https://computerhoy.com/listas/software/mejores-programas-gratis-controlar-tu-escritorio-remoto-69563
https://www.xataka.com/basics/programas-escritorio-remoto

de internet gracias al Escritorio Remoto de Chrome (o Chromium). Podemos ver el vídeo de instalación y uso en cualquiera de las siguientes direcciones:

https://www.youtube.com/watch?v=P7xMQNB_9u0
https://www.youtube.com/watch?v=YPAISPZC20U
https://www.youtube.com/watch?v=EGVhxS1t9yU

Es posible acceder al Escritorio Remoto de Chrome desde un equipo de cómputo conectándose a internet. Para acceder a un equipo de cómputo de forma remota desde un dispositivo móvil, es necesario ingresar a la cuenta personal de Google (@ciencias.unam.mx o @gmail.com) y descargar la aplicación: Escritorio Remoto de Chrome.

Configurar el acceso remoto a tu equipo de cómputo Puedes configurar el acceso remoto a tu equipo de cómputo Mac, Windows o Linux siguiendo estos pasos:

1.- Abre Chrome en tu equipo de cómputo.

2.- Escribe: remotedesktop.google.com/access en la barra de direcciones y pulsa: Enter.

3.- En la opción: "Configurar el acceso remoto" y selecciona: "Descargar".

4.- Sigue las instrucciones que aparecen en pantalla para descargar e instalar el Escritorio Remoto de Chrome.

Puede que tengas que escribir la contraseña de tu equipo de cómputo para que el Escritorio Remoto de Chrome pueda acceder. También es posible que se te pida que cambies la configuración de seguridad en Preferencias.

A continuación veremos cómo compartir tu ordenador con otro usuario para utilizar el Escritorio Remoto de Chrome.

Compartir tu equipo de cómputo con otro usuario Puedes permitir que otros usuarios accedan de forma remota a tu equipo de cómputo. Tendrán acceso completo a tus aplicaciones, archivos, correos electrónicos, documentos e historial.

1.- Abre Chrome en tu equipo de cómputo.

2.- Escribe: remotedesktop.google.com/support en la barra de direcciones y pulsa: Enter.

3.- En "Recibir asistencia" y selecciona: "Descargar".

4.- Sigue las instrucciones que aparecen en pantalla para descargar e instalar el Escritorio Remoto de Chrome.

5.- En la opción: "Recibir asistencia", selecciona: "Generar código".

6.- Copia el código y envíaselo a la persona que quieras que tenga acceso a tu equipo de cómputo -el código tiene una vigencia máxima de 5 minutos-.

7.- Cuando esa persona introduzca tu código de acceso en el sitio Web, se te mostrará un cuadro de diálogo con su dirección de correo electrónico. Selecciona la opción: "Compartir", para permitirle el acceso completo a tu equipo de cómputo.

8.- Para finalizar la sesión compartida, selecciona: "Dejar de compartir".

El código de acceso solo funcionará una vez. Cuando compartas tu equipo de cómputo, se te pedirá que confirmes que quieres seguir compartiéndolo cada 30 minutos.

Acceder a un equipo de cómputo de forma remota

1.- Abre Chrome en un equipo de cómputo.

2.- Escribe: remotedesktop.google.com/access en la barra de direcciones y pulsa: Enter.

3.- Haz clic en la opción: "Acceder" para seleccionar el equipo de cómputo que quieras.

4.- Introduce el PIN necesario para acceder a otro equipo de cómputo.

5.- Selecciona la flecha para conectarte.

Para tu protección, todas las sesiones de escritorio remoto están completamente cifradas.

Detener una sesión remota Cuando hayas terminado, cierra la pestaña para detener la sesión. También puedes seleccionar: "Opciones Desconectar".

Quitar un equipo de cómputo de la lista

1.- Abre Chrome en un equipo de cómputo.

2.- Escribe: remotedesktop.google.com/access en la barra de direcciones y pulsa: Enter.

3.- Junto al equipo de cómputo que quieras quitar, y selecciona: "Inhabilitar conexiones remotas".

Ofrecer asistencia remota

1.- Si alguien ha compartido contigo su código de acceso remoto, puedes ofrecerle asistencia de forma remota.

2.- Abre Chrome en un equipo de cómputo.

3.- Escribe: remotedesktop.google.com/access en la barra de direcciones y pulsa: Enter.

4.- En la opción: "Proporcionar asistencia", introduce el código y selecciona: "Conectar".

13.1.2 Escritorio Remoto de Windows

¿Cómo ayudar a alguien a resolver problemas en Windows accediendo y controlando su equipo de cómputo de forma remota sin instalar nada?

"Asistencia rápida" (o Quick Assist) es una utilidad del propio sistema operativo que viene integrada hace algún tiempo en Windows. Permite a dos personas compartir un equipo mediante conexión remota al estilo de *Team Viewer* y herramientas similares, pero sin necesidad de descargar ni instalar nada adicional[131].

[131] Es necesario que ambos usuarios cuenten con una cuenta de Microsoft. Si requieres generar una cuenta, lo puedes hacer en:
https://account.microsoft.com/account?lang=es-es

Cómo Usar la Asistencia Rápida de Windows Asistencia rápida es probablemente una de las herramientas más fáciles de usar que te vas a encontrar, está diseñada especialmente para proporcionar apoyo técnico a alguien con pocos conocimientos informáticos y su uso es sencillo.

Lo mejor de todo es que ya viene instalada en Windows, así que no tendrás que indicarle demasiados pasos complicados a la persona a la que quieres ayudar y esta no tendrá que descargar nada:

- Lo primero es sentarse frente a la computadora, tanto la persona que va a ofrecer ayuda como la que va a recibirla deben ejecutar la aplicación. Solo es cuestión de presionar la tecla de Windows, escribir: "Asistencia rápida" y presionar: Enter.

- Lo siguiente es seleccionar en cada equipo de cómputo cuál será el rol de cada uno. Primero la persona que va a ayudar debe seleccionar: "Ayudar a otra persona" y seleccionar el botón azul en la parte inferior.

- Después deberá iniciar sesión con su cuenta de Microsoft y una vez hecho esto aparecerá un código de seguridad de seis dígitos mismo que tendrá que compartir con la persona a la que va a ayudar.

- Por razones de seguridad ese código solo será válido durante los próximos 10 minutos. Así que antes de que acabe ese tiempo, deberás compartir el código con la persona que recibe ayuda desde su casa y esta deberá ingresarlo en el cajón de: "Asistencia rápida" justo debajo de donde dice: "Obtener asistencia".

- Una vez hecho esto la persona que ofrece ayuda tendrá que seleccionar entre dos opciones: tomar el control total del equipo de cómputo o solo ver la pantalla. La primera le permitirá usar el equipo de cómputo de la otra persona como si estuviese frente a él, la segunda solo le deja mirar qué está pasando sin poder interactuar.

- Cuando el ayudante haya elegido una opción, la persona que recibe ayuda deberá confirmar que está dando permiso para que se vea su pantalla o se controle su equipo de cómputo.

- En la ventana aparecerá el nombre de usuario que la persona que ayuda tiene en su cuenta de Microsoft, y al final solo hay que hacer Click en el botón: "Permitir".

- Si el que recibe ayuda completa los permisos, de inmediato en el escritorio de Windows de quien asiste aparecerá una ventana con el escritorio de la persona a la que ayuda, con o sin control de este dependiendo de lo que se haya elegido.
- Asistencia rápida también permite abrir una pequeña ventana de Chat para enviar indicaciones a la otra persona. La resolución de pantalla del anfitrión se escala de forma automática cada vez que redimensiones la ventana y en general funciona sumamente bien y es muy responsivo.
- Quien recibe ayuda puede detener la "Asistencia rápida" en cualquier momento, solo tiene que presionar a: "X" en el mensaje que le indica que el uso compartido de pantalla está activado. También es posible pausar la sesión en lugar de terminarla del todo.

Si en estos tiempos de trabajo remoto y confinamiento necesitas ayudar a alguien qué esta lejos, si ambos tienen Windows esta es sin duda una herramienta extremadamente útil y poderosa.

13.2 Escritorio Virtual

Las plataformas de escritorio remoto son como decimos una excelente solución para tareas de administración y asistencia remota, pero estas soluciones pueden quedarse cortas si queremos ir a un objetivo más ambicioso: el de poder trabajar con un escritorio remoto virtual.

Como habíamos visto anteriormente, eso es lo que ofrecen las plataformas de escritorio virtual y variantes como las plataformas DaaS (Desktop as a Service). Estas últimas son simplemente una implementación VDI (Virtual Desktop Infraestructure) sobre la nube.

La diferencia entre ellas dos es que usando un VDI una empresa u organización puede implementar escritorios virtuales desde sus centros de datos locales y son sus técnicos los que deben implementar y gestionar esa infraestructura. Con DaaS todo se basa en la nube y no es necesario adquirir Hardware, porque otra empresa proporciona tanto los servidores como la plataforma, su gestión y su mantenimiento.

En estas plataformas la idea es siempre la misma: ofrecer a los usuarios acceso a un escritorio virtual alojado en la nube. Pueden acceder a ese "equipo de cómputo virtual" desde cualquier otro dispositivo (otro equipo de cómputo más o menos potente, un móvil, una tableta), y trabajar en

cualquier dispositivo, por modesto que sea, con el entorno y las aplicaciones que la empresa ha puesto a disposición de sus usuarios en esos equipos de cómputo virtuales.

Las ventajas para las empresas son numerosas: los usuarios o empleados pueden acceder a sus sesiones de trabajo desde cualquier sitio y dispositivo, las empresas ahorran recursos a la hora de actualizar y mantener la infraestructura que es utilizada en los puestos de trabajo.

Además, ese tipo de escritorios virtuales garantizan un acceso seguro a todas las aplicaciones -sin que el usuario tenga que usar equipos propios que también pueda tener para uso personal- y de esta manera los usuarios no tienen que preocuparse de las actualizaciones o de instalar nuevas aplicaciones. La gestión está centralizada, es mucho más sencilla y homogénea, además de ser totalmente escalable y adaptarse dinámicamente a las necesidades de la empresa, también incluye temas muy importantes como el de la realización de copias de seguridad.

13.2.1 Escritorios y Máquinas Virtuales con VNC

Con el propósito de que el usuario que tenga acceso a un equipo de cómputo, tableta, teléfono inteligente, Chromebook o dispositivo conectado a la red, pueda usar los ambientes computacionales que se tienen instalados en un equipo determinado, se ha desarrollado el servidor de computación virtual en red VNC[132] (Virtual Network Computing) que permite visualizar la salida gráfica (de un sistema operativo en múltiples equipos o diversos sistemas operativos en un mismo equipo) por medio de red, aún si la velocidad de conexión es baja.

VNC es un programa de Software libre basado en una estructura cliente-servidor que permite interactuar con el servidor remotamente a través de

[132] Si requiere de información adicional de algunos clientes de VNC (para Windows, Linux, MacOS, Android, Raspberry PI, IOS, Chrome, Solaris, HP-UX, AIX) puede consultarlos en:
https://www.realvnc.com/es/connect/download/vnc/
https://www.geckoandfly.com/23203/vnc-client-viewer-windows-mac-linux/
https://lifehacker.com/the-best-vnc-client-for-android-5838717
https://www.tecmint.com/best-remote-linux-desktop-sharing-Software/
https://www.lifewire.com/vnc-free-software-downloads-818116
https://thelinuxcode.com/vnc-viewer-client/
https://www.howtogeek.com/142146/how-to-use-google-chrome-to-remotely-access-your-computer/

un dispositivo que disponga de un cliente VNC (Windows, Linux, MacOS, Android, Raspberry PI, iOS, Chrome, Solaris, HP-UX, AIX) o bien usando algún navegador Web (con seguridad WSS) si la salida VNC se manda como HTML (se puede usar por ejemplo el paquete noVNC) compartiendo la pantalla, teclado y ratón, sin imponer restricciones del equipo servidor con respecto al del cliente (también conocido como Computación en la Nube).

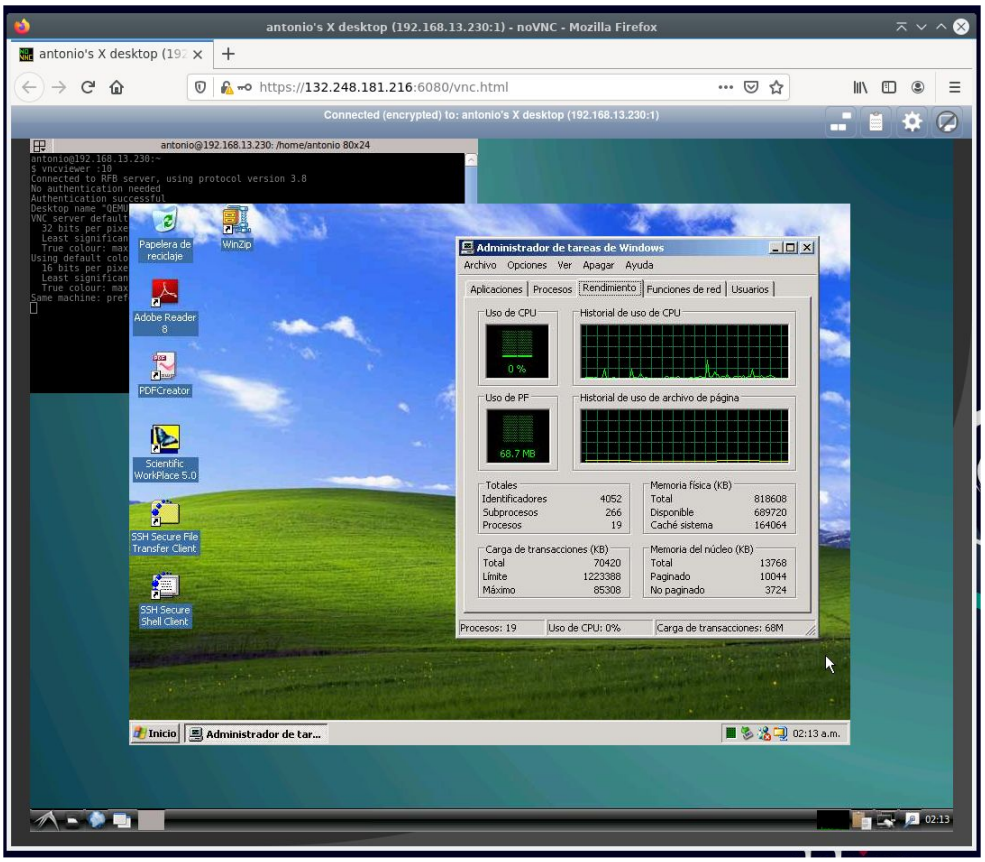

Figura 4: Uso de noVNC desde el navegador Mozilla Firefox sobre un equipo en red que soporta ejecución de máquinas virtuales sobre Debian GNU/Linux.

Cualquier equipo puede convertirse en un servidor de VNC, instalando alguna aplicación como: TigerVNC, RealVNC, Connections, TeamViewer, Remmina, NoMachine, Apache Guacamole, XRDP, FreeNX, X2Go, XPra,

AnyDesk, Krdc, Krfb, Vino, vnc4server, x11vnc, tigervnc-viewer, Vinagre, Desktopable, Ammyy Admin, Gnome-rdp, entre otros.

Para mostrar cómo trabajar con uno, usaremos tightvncserver, es ligero y se instala facilmente en Debian GNU/Linux, mediante:

```
# apt install tightvncserver
```

no requiere ninguna configuración adicional por parte del administrador (para este ejemplo supondremos que la IP del servidor es 192.168.13.230). Para compartir una sesión del usuario mediante VNC (sin cifrado) en el servidor (usando por ejemplo el puerto 30[133]) escribimos:

```
$ vncserver :30
```

la primera vez pedirá la clave de acceso (de 8 caracteres) y su confirmación, además si así lo queremos podemos generar otra clave de acceso para que se vea el escritorio en modo de solo lectura (se pueden usar para que por ejemplo, múltiples alumnos vean en distintos equipos lo que se hace en el escritorio principal sin que interfieran en él). En caso de que el puerto esté ocupado, usamos otro e intentaremos nuevamente levantar el servidor.

Cada usuario puede lanzar tantos escritorios remotos como sea necesario usando distintos puertos en el servidor de VNC, en cada uno de ellos verá un escritorio propio, pero compartirán el directorio de trabajo así como la clave de acceso.

Después de seguir estos pasos, ya es posible conectarse desde cualquier equipo con algún cliente de VNC, usando el puerto seleccionado. Por ejemplo en Debian GNU/Linux[134], si se instala como cliente de VNC a xtightvncviewer mediante:

```
# apt install xtightvncviewer
```

entonces podemos ver el escritorio compartido, usando:

[133] El puerto a usar está dentro del rango 0 en adelante -0 equivale al puerto físico 5900-.

[134] Para poder interactuar con el escritorio remoto o máquina virtual mediante VNC en Windows es necesario bajar e instalar algún cliente, por ejemplo alguno de estos paquetes:

https://www.realvnc.com/es/connect/download/vnc/windows/
https://www.tightvnc.com/

```
$ vncviewer 192.168.13.230:30
```

cuando ya no se necesite el servidor de VNC, se debe finalizar el servidor de VNC del puerto levantado, mediante:

```
$ vncserver -kill :30
```

¿Qué se puede o no se puede hacer en VNC? Desde un equipo remoto se puede hacer casi cualquier cosa -salvo escuchar el audio aunque hay proyectos trabajando en ello- que sea posible hacer sentado delante de un equipo, así como utilizar el teclado y el ratón. No se pueden controlar de forma remota dispositivos Apple iOS y Android desde un equipo de escritorio, aunque sí lo contrario.

En el equipo GNU/Linux se pueden crear cuentas individuales, compartidas y para grupos de trabajo. Además de emular diversas arquitecturas (x86_64, PowerPC, Sparc32 y 64, MIPS, ARM, ColdFire, Cris, MicroBlaze, SH4, Xtensa, entre otros) y sus respectivos procesadores; permitiendo la ejecución de máquinas virtuales para ser usadas en forma monousuario o multiusuario.

Para proporcionar el servicio de VNC usamos TigerVNC (*tightvncserver*), es una implementación de VNC neutra, independiente, de alto rendimiento y de código abierto. Es una aplicación cliente-servidor que permite a los usuarios iniciar e interactuar con aplicaciones gráficas en máquinas remotas y/o máquinas virtuales basadas en QEMU/KVM.

A diferencia de otros servidores VNC como *VNC X*, *Vino* o *Connections* que se conectan directamente con el escritorio en tiempo de ejecución, *tigervnc-vncserver* utiliza un mecanismo diferente que configura un escritorio virtual independiente para cada usuario. Es capaz de ejecutar aplicaciones de vídeo y 3D, tratando de mantener una interfaz de usuario coherente y reutilizar componentes, donde sea posible, a través de las diversas plataformas que admite. Además, ofrece seguridad a través de una serie de extensiones que implementan métodos avanzados de autenticación y cifrado TLS.

Usando VNC en GNU/Linux Por ejemplo, el usuario que disponga de una cuenta en algún servidor o que instale GNU/Linux, puede usar máquinas virtuales y compartir su escritorio de forma remota[135] sin cifrado o con él.

[135] Si no contamos con una IP pública fija homologada y deseamos dar acceso a nuestro equipo de cómputo fuera de nuestra red, será necesario instalar y configurar una Virtual

Por ejemplo, usaremos tightvncserver como servidor de VNC, lo instalamos usando:

```
# apt install tightvncserver
```

y a xtightvncviewer como cliente de VNC, lo instalamos usando:

```
# apt install xtightvncviewer
```

Uso de VNC sin Cifrado para hacer uso de VNC sin cifrado (y mayor velocidad en la transmisión), hay que acceder al servidor remoto usando SSH[136] o MOSH[137] (suponiendo la dirección 192.168.13.230), usamos:

```
$ ssh usuario@192.168.13.230
```

Una vez iniciada la sesión, es necesario levantar el servidor de VNC, usando por ejemplo el puerto[138] 30 (equivalente al puerto físico 5930), escribimos:

```
$ vncserver :30[139]
```

Private Network VPN (Red Privada Virtual) como OpenVPN.

[136] SSH (o Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un "anfitrión" (Host) remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener acceso a nuestros datos.

[137] MOSH (Mobile Shell) como medio de conexión (no corta la comunicación por inactividad como SSH), lo podemos instalar usando:

```
# apt install mosh
```

y su uso es similar al de SSH:

```
$ mosh usuario@192.168.13.230
```

[138] El puerto a usar está dentro del rango 0 en adelante -0 equivale al puerto físico 5900-.

[139] Podemos cambiar el tamaño de la ventana del cliente de VNC, además por omisión se usan 32 bits por cada Pixel, esto puede resultar muy pesado para conexiones de internet lentas, por ello se sugiere usar 24, 16 u 8 bits por Pixel, indicándolo de la siguiente forma:

```
$ vncserver -geometry 1280x768 -depth 16 :30
```

la primera vez pedirá la clave de acceso (de 8 caracteres) y su confirmación, además si así lo queremos podemos generar otra clave de acceso para que se vea el escritorio en modo de solo lectura (se pueden usar para que por ejemplo, múltiples alumnos vean en distintos equipos lo que se hace en el escritorio principal sin que interfieran en él). En caso de que el puerto esté ocupado, usamos otro e intentaremos nuevamente levantar el servidor.

Cada usuario puede lanzar tantos escritorios remotos como sea necesario usando distintos puertos en el servidor de VNC, en cada uno de ellos verá un escritorio propio, pero compartirán el directorio de trabajo así como la clave de acceso.

Después de seguir estos pasos, ya es posible conectarse desde cualquier equipo con algún cliente de VNC, usando el puerto 30:

```
$ vncviewer 192.168.13.230:30
```

Cuando ya no se necesite el servidor de VNC, hay que conectarse de nuevo al servidor remoto y finalizar el servidor de VNC del puerto o puertos levantados, usando:

```
$ vncserver -kill :30
```

Uso de VNC con Cifrado en la máquina en la que se usará el cliente de VNC, lanzamos la tunelización del cliente usando SSH (suponiendo la dirección 192.168.13.230), mediante:

```
$ ssh -L 5930:localhost:5930 –C N -f -l usuario 192.168.13.230
```

y accedemos al servidor usando SSH, mediante:

```
$ ssh usuario@192.168.13.230
```

ahora debemos lanzar el servidor VNC, pero este debe ser sólo local al servidor, si usamos el puerto[140] 30, entonces usamos:

```
$ vncserver -localhost :30[141]
```

[140] El puerto a usar está dentro del rango 0 en adelante -0 equivale al puerto físico 5900-.

[141] Podemos cambiar el tamaño de la ventana del cliente de VNC, además por omisión se usan 32 bits por cada Pixel, esto puede resultar muy pesado para conexiones de internet lentas, por ello se sugiere usar 24, 16 u 8 bits por Pixel, indicándolo de la siguiente forma:

```
$ vncserver -geometry 1280x768 -depth 16 localhost :30
```

la primera vez pedirá la clave de acceso (de 8 caracteres) y su confirmación, además si así lo queremos podemos generar otra clave de acceso para que se vea el escritorio en modo de solo lectura. En caso de que el puerto este ocupado, usamos otro e intentaremos nuevamente levantar el servidor.

Cada usuario puede lanzar tantos escritorios remotos como sea necesario usando distintos puertos en el servidor de VNC, en cada uno de ellos verá un escritorio propio, pero compartirán el directorio de trabajo así como la clave de acceso.

Ahora ya podemos lanzar el cliente de VNC, mediante:

```
$ vncviewer localhost:30
```

Cuando ya no se necesite el servidor de VNC, hay que conectarse de nuevo al servidor remoto y finalizar el servidor de VNC del puerto o puertos levantados, usando:

```
$ vncserver -kill :30
```

13.3 Desde la Nube

Existen diferentes servicios Web[142] usando VNC que permiten instalar, configurar y usar cientos de sistemas operativos Linux y Unix -máquinas virtuales usando servicios Web en Debian GNU/Linux y QEMU- desde el navegador, esto en aras de que los usuarios que cuenten con algún sistema de acceso a red y un navegador puedan usar, configurar e instalar algún sistema operativo y su respectiva paquetería sin hacer instalación alguna en su equipo de cómputo, tableta o teléfono celular[143].

Una muestra de estos proyectos son: Distrotest (https://distrotest.net) y JSLinux (https://bellard.org/jslinux).

Algunas versiones listas para usar son:

[142] Cuando se trabaja desde la Web es recomendable usar el modo Privado o Incógnito para no guardar el historial de navegación, información introducida en los formularios y borrar al cerrar el navegador los datos de los sitios visitados. Pero recuerda que los sitios Web que visitamos sí guardan información de nuestra visita, nuestro proveedor de internet también guarda constancia de nuestra visita y si descargamos algo, esto no se borra al igual que el historial de descargas, además de las marcas de páginas o favoritos se conservarán al cerrar el navegador.

[143] Estos servicios son conocidos como computación en la nube (Cloud Computing).

4mLinux, AbsoluteLinux, Academix, AlpineLinux, Antergos, antiX Linux, Aptosid, ArchBang, ArchLabs, ArchLinux, Archman, ArchStrike, ArcoLinux, ArtixLinux, AryaLinux, AV Linux, BackBoxLinux, BigLinux, Bio-Linux, BlackArch, BlackLab, BlackPantherOS, BlackSlash, blag, BlankOn, Bluestar, Bodhi, BunsenLabs, ByzantineOS, Caine, Calculate Linux Desktop, CentOS, Chakra, ChaletOS, ClearOS, Clonezilla, ConnochaetOS, Cucumber, Damn Small Linux, Damn Small Linux Not, Debian, DebianEdu, deepin, DEFT, Devil-Linux, Devuan, DragonFly BSD, Dragora, DuZeru, Dyne:bolic, Edubuntu, elementaryOS, Elive Linux, Emmabuntüs, Emmi OS, Endless OS, EnsoOS, Exe GNU/Linux, ExTiX, Fatdog64, Fedora Atomic, Fedora Server, Fedora Workstation, FerenOS, FreeBSD, FreeDOS, Frugalware, G4L, GeckoLinux, Gentoo, GNewSense, GoboLinux, Gparted, GreenieLinux, GRML, GuixSD, Haiku, Heads, Kali Linux, Kanotix, KaOS, Knoppix, Kodachi, KolibriOS, Korora, Kubuntu, Kwort, Linux Lite, Linux Mint, LiveRaizo, LMDE, Lubuntu, LXLE OS, Macpup, Mageia, MakuluLinux, Manjaro, Matriux, MauiLinux, MenuetOS, MinerOS, MiniNo, Modicia, Musix, MX Linux, Nas4Free, Neptune, NetBSD, Netrunner, NixOs, NST, NuTyX, OpenIndiana, OpenMandriva, openSUSE, OracleLinux, OSGeo live, OviOS, Parabola CLI, Parabola LXDE, Pardus, Parrot Home, Parrot Security, Parrot Studio, Parsix, PCLinuxOS, PeachOSI, Pentoo, Peppermint, PeppermintOS, Pinguy, PinguyOS, plopLinux, PointLinux, Pop!_OS, PORTEUS, Puppy Linux, PureOS, Q4OS, QubesOS, Quirky, Raspberry Pi Desktop, ReactOS, Redcore, Rescatux, RevengeOS, RoboLinux, Rockstor, ROSA FRESH, Runtu, Sabayon, SalentOS, Salix, ScientificLinux, Siduction, Slackware, Slax, SliTaz, Solus, SolydK, SolydX, SparkyLinux, Springdale, StressLinux, SubgraphOS, SwagArch, Tails, Tanglu, Tiny Core, Trisquel, TrueOS, TurnKey Linux, Ubuntu, Ubuntu Budgie, Ubuntu Studio, UbuntuKylin, Uruk, VectorLinux, VineLinux, VoidLinux, Voyager, VyOS, WattOs, Xubuntu, Zentyal, Zenwalk, Zevenet, Zorin OS

Terminales de Linux en la Web

- https://www.tutorialspoint.com/execute_bash_online.php
- http://www.webminal.org/
- https://bellard.org/jsLinux/
- https://codeanywhere.com/
- https://copy.sh/v86/
- https://www.masswerk.at/jsuix/
- https://linuxcontainers.org/lxd/try-it/
- http://cb.vu/

Editores BAHS en la Web

- https://www.shellcheck.net/
- https://www.learnshell.org/
- https://www.tutorialspoint.com/execute_bash_online.php
- https://paiza.io/en/projects/new?language=bash
- https://www.jdoodle.com/test-bash-shell-script-online
- http://rextester.com/l/bash_online_compiler

Windows 365 Microsof presentó en julio del 2021 la nueva versión de Windows en la nube que llevará el nombre de Windows 365. Este nuevo servicio de suscripción, está especialmente dirigido a empresas, que permitirá acceder a nuestra sesión de usuario desde cualquier equipo (el PC, el Mac, la tableta o teléfono Android, etc.), pues el Software y el sistema de archivos estarán alojados en una máquina virtual remota, por lo que la confi-guración, documentos y herramientas disponibles serán idénticos desde donde accedamos.

Así, desde cualquier navegador (o bien usando la aplicación de Escritorio Remoto de Windows) podremos acceder a un Windows 10/11 disfrutando de una experiencia de arranque casi instantáneo, pero esa no será la única ventaja de esta plataforma. Aún más importante será la posibilidad de contar con varios 'ordenadores' en una misma cuenta, cada uno con distinta potencia (RAM, núcleos de procesador...) y capacidad de almacenamiento contratada, según el trabajo que necesitemos llevar a cabo en cada momento.

Microsoft ya ha confirmado que ofrecerá 12 configuraciones de Hardware distintas para sus equipos virtualizados (iniciando en $130 pesos mexicanos por mes). Así, las empresas podrán 'crear PCs' en cuestión de minutos y asignar cada uno a un empleado, eliminando los inconvenientes que conlleva el hecho de manejar Hardware físico.

14 Bibliografía

Este texto es una recopilación de múltiples fuentes, nuestra aportación -si es que podemos llamarla así- es plasmarlo en este documento, en el que tratamos de dar coherencia a nuestra visión de los temas desarrollados.

En la realización de este texto se han revisado -en la mayoría de los casos indicamos la referencia, pero pudimos omitir varias de ellas, por lo cual pedimos una disculpa- múltiples páginas Web, artículos técnicos, libros, entre otros materiales bibliográficos, los más representativos y de libre acceso los ponemos a su disposición en la siguiente liga:

Herramientas
http://132.248.181.216/Herramientas/

Referencias

[1] https://es.wikipedia.org/wiki/Microsoft_Windows 83

[2] https://es.wikipedia.org/wiki/Linux 97

[3] https://es.wikipedia.org/wiki/Unix 90

[4] https://es.wikipedia.org/wiki/Berkeley_Software_Distribution 90

[5] https://es.wikipedia.org/wiki/Mac_OS 94

[6] https://es.wikipedia.org/wiki/Android 111

[7] https://www.gnu.org/philosophy/free-sw.es.html 337

[8] https://es.wikipedia.org/wiki/Software_libre 337

[9] https://www.hispaLinux.es/SoftwareLibre 337

[10] https://es.wikipedia.org/wiki/Software_propietario 335

[11] Diferentes Tipos de Licencias para el Software, https://www.gnu.org/licenses/license-list.html 337, 347

[12] FSF, Free Software Fundation, http://www.fsf.org/ 337, 347, 388

[13] GNU Operating System, http://www.gnu.org/ 337, 347

[14] El economista, https://eleconomista.com.mx/tecnociencia/2013/01/22/clausuraran-negocios-mexico-uso-ilegal-Software

[15] PCworld, http://www.pcworld.com.mx/UNAM-y-BSA-promueven-el-uso-de-Software-legal/

[16] QEMU, http://wiki.qemu.org/Main_Page 379

[17] KVM, http://www.linux-kvm.org/page/Main_Page 379

[18] Oracle MV VirtualBox, https://www.virtualbox.org 395

[19] Máquinas Virtuales, http://es.wikipedia.org/wiki/Máquina_virtual 379

[20] Algunos usos de máquinas Virtuales, 379
http://www.configurarequipos.com/doc747.html

Sitios Web revisados:

- https://www.ibm.com/security
- https://www.welivesecurity.com/la-es/
- http://blogs.eset-la.com/
- http://www.criptored.upm.es/
- https://www.securityfocus.com/
- https://securiteam.com/
- https://www.cert.unam.mx/
- http://www.securitytube.net/
- https://www.issa.org/
- https://www.isaca.org/

- https://www.sans.org/
- https://www.eccouncil.org/
- https://www.isc2.org/
- https://www.comptia.org/
- http://oval.mitre.org/
- https://www.offensive-security.com/
- https://www.giac.org/certification/penetration-tester-gpen
- https://www.isecom.org/
- https://www.exploit-db.com/google-hacking-database
- https://www.ccn-cert.cni.es/
- https://www.securityfocus.com/
- https://linuxsecurity.com/
- https://www.identidadrobada.com/
- https://www.ietf.org/
- https://www.iso.org/home.html
- https://www.bis.org/bcbs/
- http://www.mit.edu/hacker/hacker.html

Declaramos terminado este trabajo sufrido, ideado y llevado a cabo entre los años 2020 al 2025, aún y a pesar de impedimentos tales como: la mala suerte, la desventura, el infortunio, la incomprensión, la gripe, el COVID-19, la migraña, las horas de frío y calor, la tristeza, la desesperanza, el cansancio, el presente, el pasado y nuestro futuro, el que dirán, la vergüenza, nuestras propias incapacidades y limitaciones, nuestras aversiones, nuestros temores, nuestras dudas y en fin, todo aquello que pudiera ser tomado por nosotros, o por cualquiera, como obstáculo en este tiempo de mentiras, verdades, de incredulidad e ignorancia o negación de la existencia real y física de la mala fe.

Atentamente

Antonio Carrillo Ledesma
Karla Ivonne González Rosas