

USERS

INCLUYE
VERSIÓN DIGITAL
GRATIS

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

HERRAMIENTAS Y TÉCNICAS PARA
PREVENIR Y COMBATIR ATAQUES A LOS
SISTEMAS INFORMÁTICOS DE UNA EMPRESA

METODOLOGÍAS Y MÉTRICAS DE SEGURIDAD

ESTÁNDARES Y PROCEDIMIENTOS

SITIOS DE CONTINGENCIA

DISEÑO DE REDES SEGURAS

DETECCIÓN DE INTRUSOS
EN SISTEMAS OPERATIVOS



GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Herramientas y técnicas para prevenir
y combatir ataques a los sistemas
informáticos de una empresa

HACKING
LATAM

Red**USERS**

USERS

TÍTULO: Gestión de la seguridad informática
AUTOR: Fabián Portantier
COLECCIÓN: Desde Cero
FORMATO: 19 x 15 cm
PÁGINAS: 192

Copyright © MMXIII. Es una publicación de Fox Andina en coedición con DÁLAGA S.A. Hecho el depósito que marca la ley 11723. Todos los derechos reservados. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Su infracción está penada por las leyes 11723 y 25446. La editorial no asume responsabilidad alguna por cualquier consecuencia derivada de la fabricación, funcionamiento y/o utilización de los servicios y productos que se describen y/o analizan. Todas las marcas mencionadas en este libro son propiedad exclusiva de sus respectivos dueños. Impreso en Argentina. Libro de edición argentina. Primera impresión realizada en Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. de Buenos Aires en XII, MMXIII.

ISBN 978-987-1949-30-4

Portantier, Fabián

Gestión de la seguridad informática. - 1a ed. - Ciudad Autónoma de Buenos Aires : Fox Andina; Buenos Aires: Dalaga, 2013.

192 p.; 19x15 cm. - (Desde cero; 33)

ISBN 978-987-1949-30-4

1. Informática. I. Título.

CDD 005.3



Prólogo al contenido

Las organizaciones de Latinoamérica tienen que incluir a la seguridad informática dentro de sus políticas de inversión, mientras que los profesionales de la seguridad debemos acostumbrarnos a implementar medidas de control adecuadas a nuestras capacidades económicas, pero basándonos en lo que dictan los estándares internacionales.

Este libro llevará al lector por un recorrido que va desde los fundamentos principales de la seguridad informática, hasta trucos específicos para los sistemas más utilizados en las infraestructuras tecnológicas de la actualidad; cuestiones que se comparten con los lectores para que puedan desenvolverse de forma rápida en el mundo de la seguridad, con una base sólida que les permitirá llevar a cabo sus tareas de la mejor manera posible.

Esta obra le será de utilidad tanto al estudiante para formar su carrera, así como también a la persona que ya se desempeña como profesional de la seguridad, y que busca perfeccionar sus conocimientos y mejorar sus aptitudes laborales. Con muchas referencias a excelentes productos y fuentes de información, el lector podrá descubrir una gran cantidad de herramientas para construir su arsenal de trabajo y tener la capacidad de dar respuesta a varias situaciones diferentes.

La seguridad informática es una de las áreas de estudio más apasionantes en la actualidad. Muchas veces es vista más como un juego que como un trabajo, debido a que requiere un proceso de aprendizaje constante, en el que, además de mejorar nuestras capacidades para asegurar sistemas y programar aplicaciones, hay lugar para la diversión. Pero más allá de eso, estamos hablando de una profesión que requiere mucho de nosotros debido, justamente, a este proceso de aprendizaje constante, que nos obliga a leer permanentemente acerca de los nuevos productos y tecnologías que se están implementando en el mercado, estar al tanto de cuáles son las metodologías más efectivas y tener en mente qué es lo que nos depara el siguiente paso del mundo de la informática.

El libro de un vistazo

Este libro nos entrega los conceptos y herramientas que necesitamos para desempeñarnos eficazmente en el ámbito de la seguridad informática. Analizaremos la mejor forma de acercarnos a esta fascinante profesión aprendiendo en detalle todo lo que debemos saber cómo expertos en seguridad.

*01



LA SEGURIDAD INFORMÁTICA

Aquí revisaremos las bases para tener una visión global de la seguridad informática, analizaremos los objetivos de la seguridad en las empresas y las metodologías que atraerán el éxito a nuestro trabajo. Aprenderemos a diferenciarnos como profesionales sin centrarnos únicamente en los aspectos técnicos, considerando temas administrativos de la profesión.

*03



CONTINUIDAD DEL NEGOCIO

Explicaremos cuáles son las tareas que debe llevar a cabo una organización para garantizar su continuidad operativa, resistir ataques y otros eventos adversos que pudieran presentarse. Algunos de los temas que trataremos serán las copias de seguridad, el monitoreo y la gestión de incidentes.

*02



GESTIÓN DE LA SEGURIDAD

En este capítulo analizaremos el proceso de gestión de la seguridad informática, entenderemos las responsabilidades que tiene cada persona dentro de la organización y veremos cómo y por qué deben redactarse los documentos formales.

*04



TELECOMUNICACIONES

En este capítulo aprenderemos a realizar un inventario de los activos de información, así como también las mejores maneras de proteger nuestros dispositivos de telecomunicaciones (como por ejemplo routers, switches y firewalls), y de qué modo utilizar estos equipos para aumentar la seguridad de nuestra red.



*05



SISTEMAS OPERATIVOS

Aquí revisaremos herramientas y técnicas usadas para asegurar los sistemas operativos GNU/Linux y Microsoft Windows, y las tecnologías relacionadas con los controles de acceso, la autenticación de usuarios centralizada, las copias de seguridad y la protección de los servicios de red que se brinda con los servidores, además de los clientes que se conectan a ellos.

*Ap

ON WEB



TENDENCIAS ACTUALES

En este capítulo realizaremos un repaso por las tecnologías que se están utilizando actualmente y de qué forma podemos protegerlas.

Algunos de los temas por tratar son la Web 2.0, voz sobre IP, virtualización y cloud computing.



INFORMACIÓN COMPLEMENTARIA

A lo largo de esta obra, podrá encontrar una serie de recuadros que le brindarán información complementaria: curiosidades, trucos, ideas y consejos sobre los temas tratados. Para que pueda distinguirlos en forma más sencilla, cada recuadro está identificado con diferentes iconos:



CURIOSIDADES
E IDEAS



ATENCIÓN



DATOS ÚTILES
Y NOVEDADES



SITIOS
WEB

Contenido del libro

Prólogo	3
Introducción	10

*01

La seguridad informática

Introducción	12
La seguridad como profesión	13
El estudio, nuestro pan de cada día.....	15
Títulos y certificaciones	17
Metodologías de trabajo	19
Defensa en profundidad	20
El principio KISS	22
Desde arriba hacia abajo	24
La seguridad en las empresas	26
La seguridad como proceso de negocio.....	27
Métricas de seguridad	30
Mejora continua	32
Resumen	33
Actividades	34

*02

Gestión de la seguridad

Introducción	36
El autoconocimiento	37
Análisis cualitativo vs. cuantitativo	41
Amenazas y vulnerabilidades	43
Implementación de controles	49
Políticas y otros documentos.....	52
Políticas	52

Estándares	54
Procedimientos	56
Responsabilidades	57
El equipo de seguridad	58
Capacitación al personal.....	60
Dueños, custodios y usuarios de datos	61
Resumen	63
Actividades	64

*03

Continuidad del negocio

Introducción	66
Copias de respaldo.....	67
Monitoreo	71
Control de cambios	74
Ambientes de pruebas y producción.....	77
Gestión de incidentes	78
BIA, BCP y DRP.....	81
Sitios de contingencia.....	86
Resumen	89
Actividades	90

*04

Telecomunicaciones

Introducción	92
Inventario de dispositivos	93
Switches inteligentes.....	93
Arpalert	93
Scripting.....	94

Routers y switches	96	Hardening	144
Port Security	98	Network Access Control.....	150
DHCP Snooping	100	Malware	152
Cuentas de acceso centralizadas.....	100	Protección en capas	155
Utilización de servidores syslog	102	Firewalls.....	155
Firewalls	103	Backups	157
Redes inalámbricas.....	106	Herramientas basadas en agentes	158
Prevención de intrusos.....	110	Herramientas sin agentes.....	159
Implementación de sistemas IDS	114	Scripts personalizados.....	159
Administración remota	114	Recuperación completa	160
CLI vs. TUI vs. GUI vs. WUI.....	117	Autenticación multifactor.....	161
Protocolos TCP/IP	119	Tokens o smart cards.....	161
SSH	120	Tokens virtuales.....	162
TLS.....	121	Tarjetas de coordenadas.....	162
SMTP, IMAP y POP3	122	Biometría	163
HTTP y FTP	123	Servidores de autenticación.....	165
DHCP.....	125	Análisis de logs	167
DNS	126	Servidores centralizados.....	168
SNMP	128	Administración remota.....	170
Diseño de redes seguras	130	Port knocking	171
Zonas desmilitarizadas.....	130	WMI	172
Separación de VLANs	134	RDP y VNC	175
Redes privadas virtuales.....	136	SSH	175
Resumen	137	SNMP.....	176
Actividades	138		

* 05

Sistemas operativos

Características.....	140
Windows vs. UNIX	141
Consejos para sistemas Windows	142
Consejos para sistemas UNIX.....	143



Webmin.....	176
Detección de intrusos.....	177
Honeypots	178
Gestión de parches	180
Resumen	181
Actividades	182



Servicios al lector

Índice temático.....	184
----------------------	-----



Ap

ON WEB

Tendencias actuales

Tecnología

Web 2.0

Redes sociales
Google hacking
Phishing y robo de identidad

Servicios de mensajería

Mensajería instantánea
Transferencia de archivos
Fuga de información
Comunicaciones no deseadas (spam)

VoIP

Espionaje de comunicaciones
Videoconferencias

Virtualización

Asegurar correctamente los equipos de host
Asegurar los medios de almacenamiento
Asegurar cada una
de las máquinas virtuales

Utilizar adecuadamente las plantillas
de máquinas virtuales

Controlar adecuadamente la gestión
de la infraestructura virtual

Implementar filtros físicos

en las zonas de alta criticidad

Los sistemas host son tan críticos como
la máquina virtual que corre sobre ellos

Separar una red para administración,
de la infraestructura virtual

Garantizar la conectividad de la infraestructura
con las demás redes

Implementar separación de tareas
para la gestión de la infraestructura

Contar con redundancia de equipos

Cloud computing

Utilizar encriptación de discos
Asegurarnos de tener copias
de respaldo de los datos
Contratar solo a proveedores de confianza
La privacidad de los datos

Diferencias con otros servicios

Tecnología móvil

Dispositivos portátiles
Teletrabajo

Ataques dirigidos

Denegación de servicio (DoS)
El peligro de la perseverancia

Expectativas para el futuro

Resumen

Actividades





Introducción

Para obtener el mayor provecho de esta obra es importante leerla de forma detenida y prestando atención en cada momento, debido a que no existe una parte o un capítulo más importante que otro, sino que, más bien, se trata de una guía que debe tenerse en cuenta de manera completa, analizando cada uno de los conceptos que aquí se exponen y buscando llevar a la práctica cada uno de los consejos mencionados.

Como podremos observar, este libro no pretende explicar en detalle cada tecnología utilizada, porque se necesitarían decenas de miles de hojas para hacerlo. En cambio, podemos afirmar que expondremos algunos de los trucos y consejos más efectivos que un profesional puede conocer. Es por eso que cada página debe considerarse parte fundamental de las enseñanzas aquí expuestas.

La obra está dividida en capítulos que se encargan de explicar los fundamentos de la seguridad y los procesos que debe tener en cuenta toda organización si quiere mantener la seguridad de sus datos. También se profundiza en las herramientas y técnicas más utilizadas para asegurar sistemas operativos, dispositivos de telecomunicaciones y las nuevas tecnologías emergentes.



La seguridad informática

En este capítulo sentaremos las bases para tener una visión global de la seguridad informática, y analizaremos los objetivos de la seguridad en las empresas y las metodologías que atraerán el éxito a nuestro trabajo. Veremos cómo diferenciarnos como profesionales sin centrarnos únicamente en los aspectos técnicos, ya que también debemos considerar los aspectos administrativos de la profesión.

▼ Introducción.....	12	▼ Métricas de seguridad.....	30
▼ La seguridad como profesión .	13	▼ Mejora continua.....	32
▼ Metodologías de trabajo	19	▼ Resumen.....	33
▼ La seguridad en las empresas .	26	▼ Actividades.....	34



Introducción

Con el correr de los años, los seres humanos dependemos cada vez más de la tecnología para mantener nuestro estilo de vida. Ya sea para que las empresas puedan desarrollar sus negocios o para que las personas realicen sus tareas cotidianas, la tecnología siempre está ahí, simplificando las cosas. Esto ha llevado a una dependencia en la que no todas son ventajas. Si nos situamos unos veinte años atrás, podemos imaginar que la pérdida de conectividad con Internet o el mal funcionamiento de un sistema resultaba algo bastante molesto. Hoy en día, la pérdida de conectividad significa que una empresa quede prácticamente inoperante.

A medida que las personas volcamos nuestras vidas hacia la tecnología, almacenamos información personal, registros médicos y balances de cuenta en sistemas informáticos. Y a medida que las organizaciones confían en la tecnología para hacer negocios, establecer comunicaciones y transferir fondos, empiezan a aparecer otras personas, no tan bien intencionadas, que la ven como una excelente plataforma para cometer acciones ilícitas, con el fin de obtener beneficios a costa de los demás. Debido a esto, los

EXISTEN PERSONAS
QUE USAN LA
TECNOLOGÍA PARA
COMETER ACTOS
ILÍCITOS



daños por robo o pérdida de información crecen a la par de nuestra dependencia tecnológica. Muchos criminales optan por utilizar la tecnología como herramienta, ya sea para cometer nuevas formas de crimen o para complementar las viejas.

No solo estamos hablando de malware y virus, sino también de programas especializados en robar información bancaria, en extraer datos personales y en realizar acciones cada vez más direccionadas al enriquecimiento ilícito. En el caso de las empresas, debemos sumar los intereses que puede llegar a tener la competencia por obtener datos confidenciales, como planes de marketing, balances financieros, datos de clientes, etcétera.



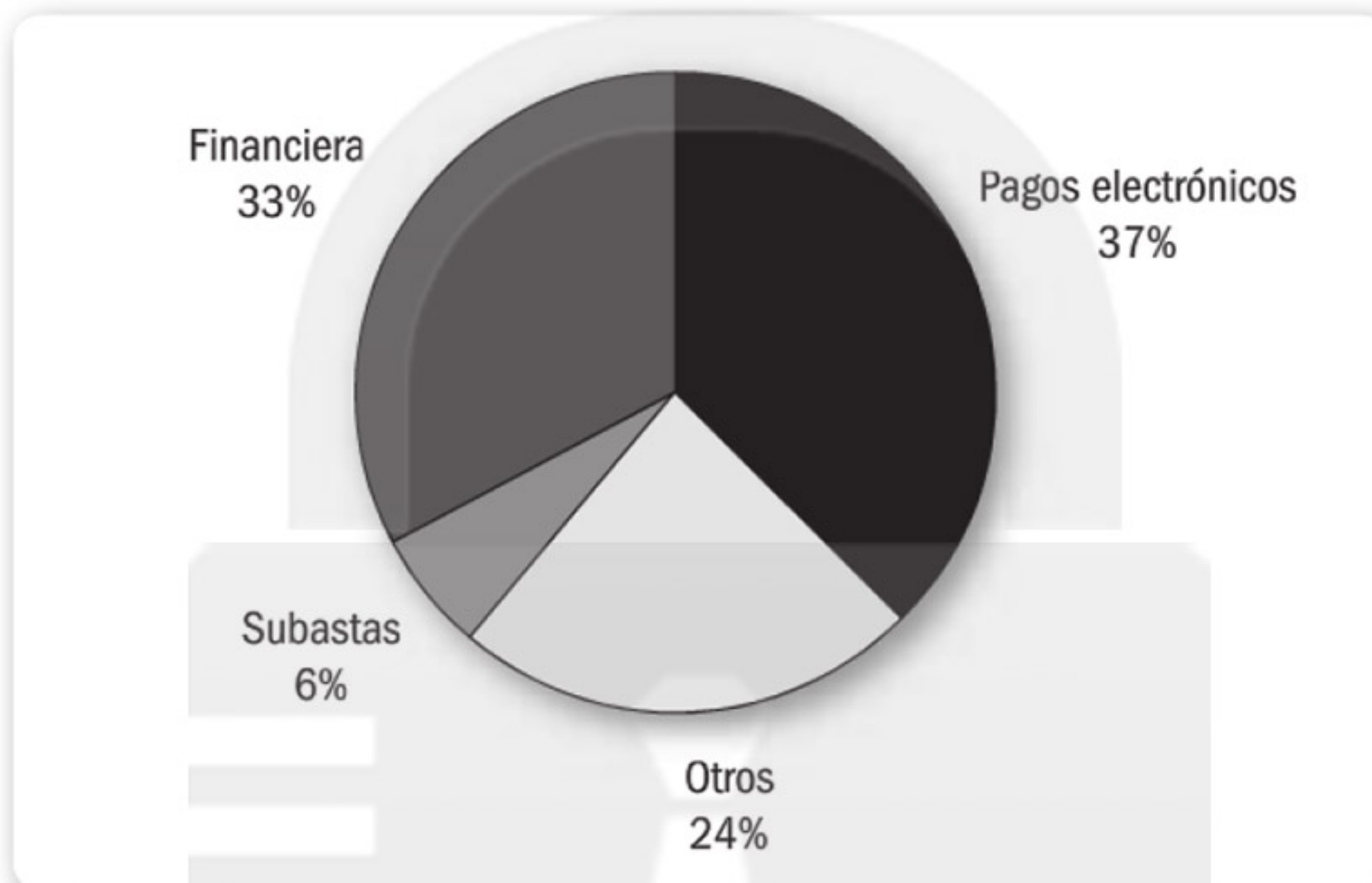


Figura 1. Si analizamos los sitios que han sufrido ataques de phishing durante 2010, vemos que los relacionados con actividades financieras fueron el principal objetivo de los criminales.

Es por eso que se ha vuelto necesario establecer mejores prácticas y crear herramientas destinadas a proteger la información de las personas y las organizaciones. Todos estos esfuerzos se conocen como **seguridad informática**, y han ido evolucionando hasta convertirse en un área de estudio que dio lugar a profesionales dedicados a proteger la información.



La seguridad como profesión

Ser un profesional de la seguridad informática es una tarea bastante particular, debido a que, como veremos en este capítulo, nos llevará a tener relación con todas las áreas de una empresa. Es imperativo que tengamos un conocimiento amplio acerca de cómo funciona la organización para la que estamos trabajando, sus procesos de negocio, sus objetivos y otros aspectos. Solo de esta manera podremos tener una visión global acerca de cómo es

adecuado proteger la información con la que trabajamos. Debemos ser objetivos en cuanto a las medidas de seguridad por implementar, considerando los intereses de la organización como nuestro principal motor de acción.

Esta es una profesión para la cual precisamos estudiar una gran cantidad de material y tener en consideración varios estándares y metodologías, lo que puede llevarnos a pensar solamente en lo que debería hacerse y a olvidarnos de lo que puede hacerse.

Lo que **debería hacerse** es exactamente lo que dice la norma **ISO 27000**. Si nos detenemos a pensar, esta es una norma escrita por profesionales destacados, con una amplia experiencia y un entendimiento claro de lo que es la seguridad de la información.

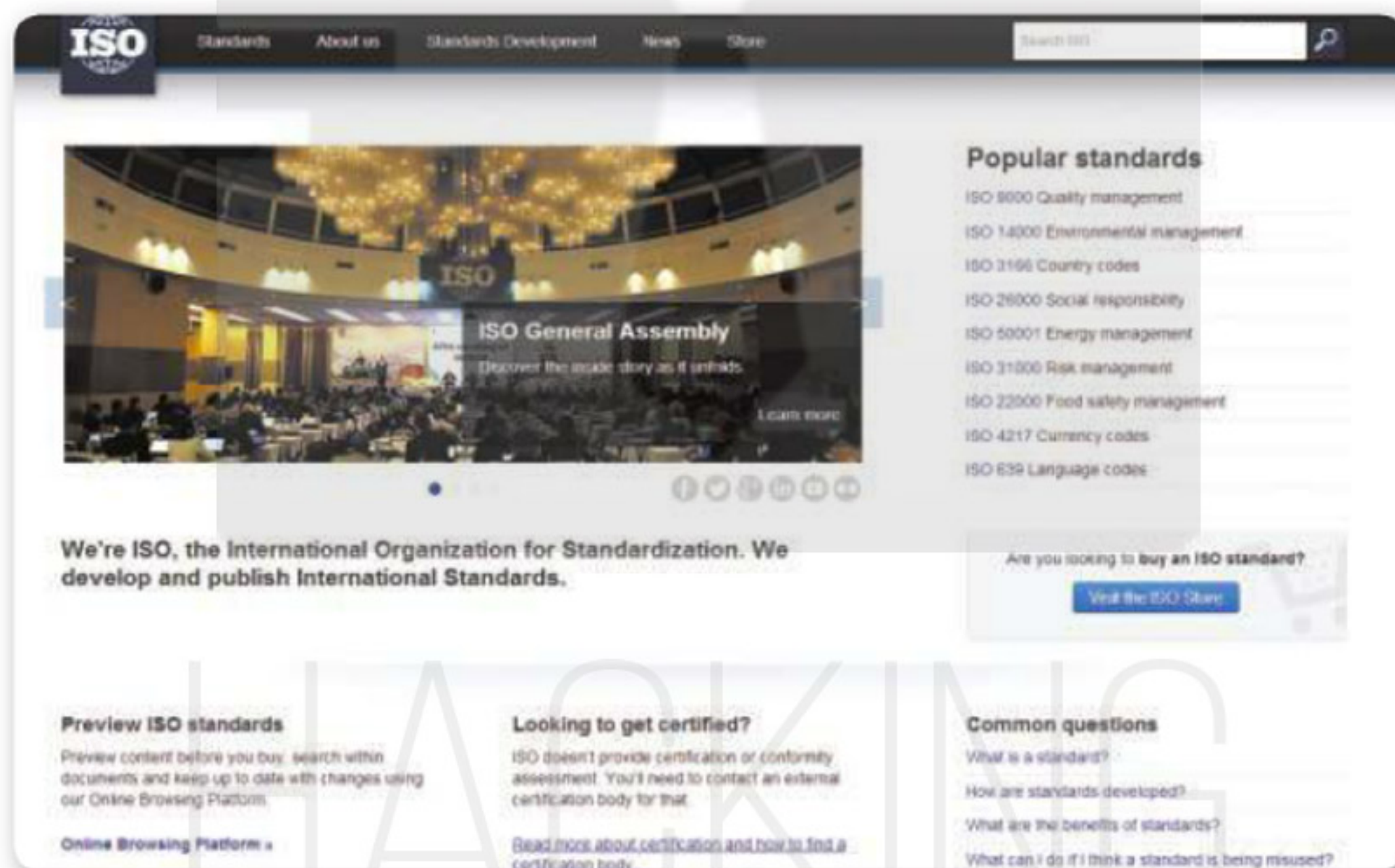


Figura 2. La principal función de ISO (www.iso.org) es buscar la estandarización de normas de productos y seguridad para las empresas y organizaciones a nivel internacional.

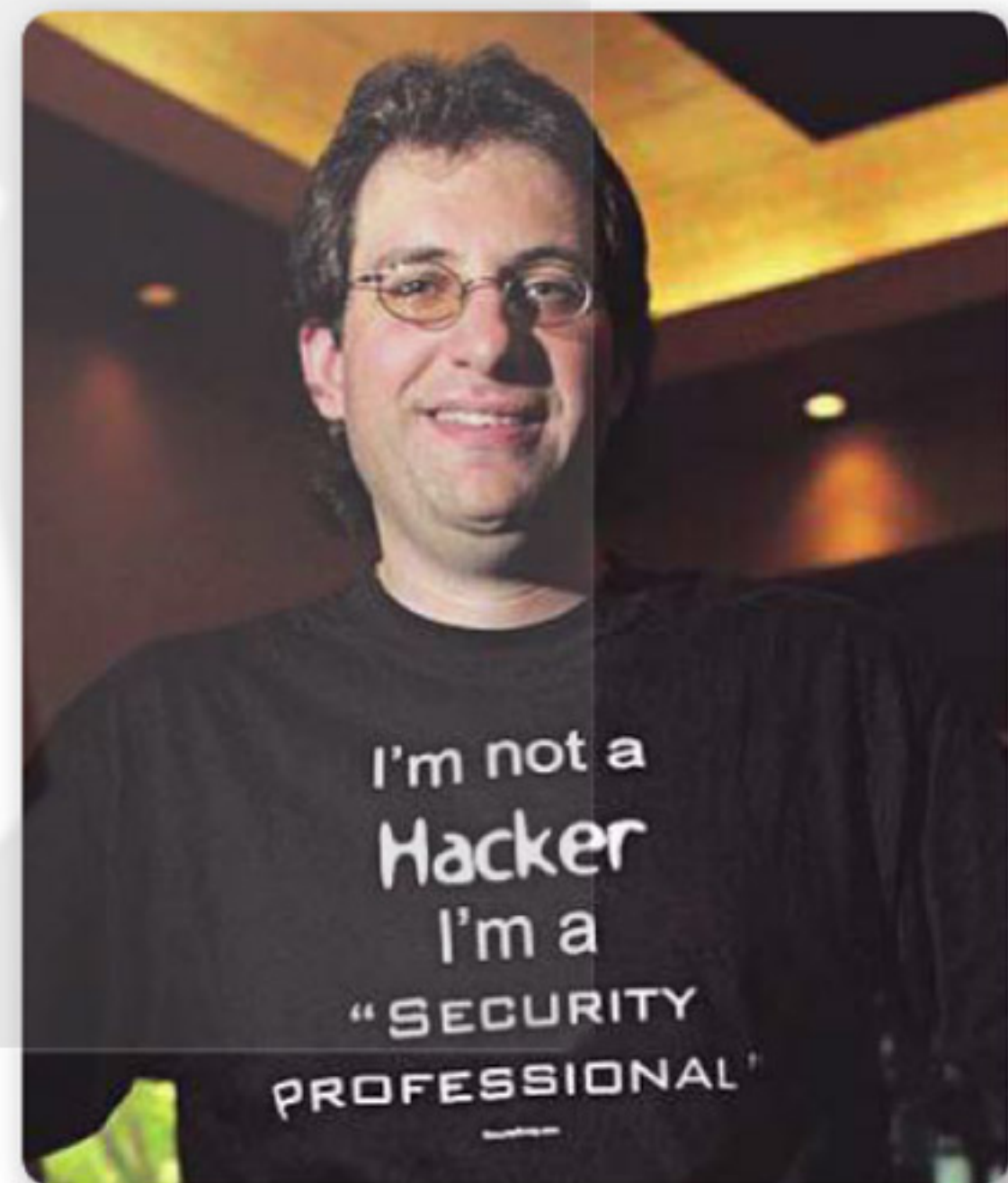
Lo que **puede hacerse** es analizar las mejores prácticas que podemos implementar, muchas veces, basándonos en normas como la ISO 27000, pero considerando que nuestros recursos son limitados. Incluso en las

organizaciones más grandes, los recursos tienen un límite; la única diferencia es la cantidad de ceros a la derecha que tienen esos límites.

Aquí entra en juego nuestra capacidad para poner los pies sobre la tierra y discernir entre lo que dice una norma de mejores prácticas acerca de todo lo que debería hacerse para proteger la información de una organización y los recursos con los que cuenta una entidad para implementar medidas de seguridad, sin entrar en quiebra por tener que realizar dichas inversiones.

Tengamos en cuenta que los objetivos de las organizaciones son variados: captar más clientes, ganar más dinero, brindar mejores servicios, tener los costos más bajos, y otros, pero no existe ninguna organización en la que el objetivo principal sea tener las mejores medidas de seguridad informática.

Figura 3. Kevin Mitnick, uno de los hackers más famosos, luego de haber pasado varios años en prisión se dedicó a brindar servicios como profesional de la seguridad y a escribir libros sobre el tema.



Nuestro trabajo en una organización es ayudarla a alcanzar sus objetivos, implementando las medidas de seguridad adecuadas para evitar pérdida de datos, robo de información y fraudes. Teniendo esto en cuenta, seremos profesionales que aporten verdadero valor a la organización y estaremos muy bien vistos en todos los niveles jerárquicos de la empresa.

El estudio, nuestro pan de cada día

Está implícito que, si hemos elegido esta carrera, tenemos una gran afición por los avances tecnológicos y el estudio de los sistemas.

Tener la capacidad de asegurar un sistema implica entender cómo funciona. Por lo tanto, es necesario estar ampliamente capacitados en varias tecnologías y mantener un estudio constante acerca de los cambios y las nuevas posibilidades que se abren año tras año.



Figura 4. El servicio gratuito **Una al día** de **Hispasec Sistemas** (www.hispasec.com), brinda un canal RSS con una noticia de seguridad diaria para mantenernos actualizados.



REDUSERS PREMIUM



Para obtener material adicional gratuito, ingrese a **Publicaciones/Libros** dentro de <http://premium.redusers.com>. Allí encontrará todos nuestros títulos y podrá acceder a contenido extra, como sitios web relacionados, programas recomendados, ejemplos utilizados por el autor, apéndices y archivos editables o de código fuente. Todo esto ayudará a comprender mejor los conceptos desarrollados en la obra.

En varias carreras, para tener éxito necesitaremos alcanzar algo que se llama **superespecialización**. Esto quiere decir que tendremos un conocimiento extremadamente avanzado acerca de un tema específico. Por ejemplo, hay profesionales que están superespecializados en **tecnologías de storage**. Esto les permite ser de primer nivel y tener la capacidad de solucionar prácticamente cualquier tipo de problemas que pueda surgir dentro de su área de estudio.

En el caso de la seguridad informática, la superespecialización no sirve. Estamos hablando de una carrera en la que necesitamos trabajar con todas las tecnologías que utiliza una organización: las redes, los sistemas operativos, el storage, las aplicaciones, etcétera. No podemos ser expertos en todo sino que será preferible tener un entendimiento amplio de cada una de estas tecnologías. Esto nos dará una visión abarcativa de toda la infraestructura tecnológica, y tendremos la capacidad de implementar soluciones de seguridad para toda la organización, teniendo en cuenta la totalidad de los aspectos que la afectan.

Títulos y certificaciones

La industria tecnológica tiene la particularidad de que no es necesario contar con títulos o certificaciones que avalen nuestros conocimientos para que podamos ser profesionales. Si bien este tipo de reconocimientos puede abrirnos las puertas a diferentes oportunidades laborales, no son totalmente necesarios.



ACTUALIZARSE SIEMPRE



Capacitarnos mantiene nuestros cerebros receptivos a nuevos conocimientos y experiencias. A medida que pasa el tiempo será más fácil leer documentación técnica y tendremos la capacidad de deducir cosas no explicadas gracias a la experiencia y a que el diseño de los sistemas sigue patrones comunes que se repiten en la mayoría de las soluciones.

Al tomar otras carreras como ejemplo, ya sea la medicina, la abogacía o la contaduría, vemos que todas requieren, obligatoriamente, el título de grado para poder ejercer. Ante esto, muchas veces surge el interrogante de si es necesario o no poseer certificaciones que acrediten nuestras competencias profesionales. Aquí, como en muchas otras cuestiones, la respuesta es “depende”. Siempre debemos tener en cuenta el costo y el beneficio asociado a tener una acreditación. El costo puede ser económico, el tiempo de estudio que nos demande, etcétera. También debemos considerar el cargo profesional al que apuntamos, debido a que en ciertas organizaciones, es imprescindible tener un título para obtener trabajo. Puntualmente, en la seguridad informática se habla más de certificaciones que de títulos de grado, por ser estas más flexibles y estar más actualizadas. En caso de

que queramos diferenciarnos del resto, y de acuerdo con el perfil profesional que busquemos, podemos optar por diferentes certificaciones. Algunas de ellas son **CISSP**, **Security+**, **CISA**, **CISM** y **CEH**, entre otras.



Figura 5. CISSP (www.isc2.org)

es considerada como una de las credenciales de mayor representatividad en el ámbito de la seguridad informática a nivel mundial.

Otro punto importante, que muchos profesionales dejan de lado, es el dominio del idioma inglés. Este es necesario para comprender la mayoría de la documentación existente sobre seguridad. Si tenemos problemas para dominar este idioma, estaremos muy limitados en cuanto a las fuentes de información de las que podemos nutrarnos. Es importante que contemos con la capacidad de leer en inglés, aunque podemos dejar de lado el hecho de hablar y escribir, tareas no tan necesarias para el estudio.

También son valables nuestra capacidad para resolver problemas, el hecho de poder brindar las mejores soluciones e implementar correctamente las medidas de seguridad, ya que esto nos diferenciará como profesionales de primer nivel. Tengamos en cuenta que contar con una certificación garantiza que tenemos nociones acerca de ciertos tipos de conocimientos, pero el no contar con una no quiere decir que no los tengamos. Lo más importante siempre será nuestra aptitud y nuestros conocimientos, más allá de cualquier título que podamos tener.



Metodologías de trabajo

Como toda área de estudio en desarrollo, la seguridad informática ha ido mutando con el correr del tiempo. Fue necesario crear nuevas tecnologías específicas para la protección de los datos con la misma frecuencia con la que se crean las tecnologías que estamos encargados de proteger. Pero, más allá de que podamos evolucionar constantemente generando nuevos mecanismos de defensa, es necesario que contemos con bases sólidas sobre las que podamos trabajar.

Estas bases son las metodologías que utilizamos para realizar nuestras tareas, y debemos pensar en ellas como los fundamentos de cada una de nuestras acciones.



OTRAS FUENTES DE INFORMACIÓN



Para conocer más acerca de las certificaciones de seguridad más importantes, podemos visitar sus sitios web correspondientes:

- * CISSP (www.isc2.org)
- * CEH (www.eccouncil.org)
- * Security+ (www.comptia.org)

Es preciso ubicar estos conceptos en un nivel amplio, sin ser específicos sino más bien globales, para que nos marquen los lineamientos acerca de cómo debemos proceder. En las siguientes páginas analizaremos varias metodologías que podemos implementar para aumentar nuestra productividad y destacarnos como profesionales de primer nivel.

Defensa en profundidad

Como la seguridad informática es una ciencia tan innovadora y evolutiva, suele plantear nuevas maneras de hacer las cosas. Pero existe una metodología implementada en todo el mundo que nadie pone en discusión y siempre se promueve como la mejor: la **defensa en profundidad**, que apunta a implementar varias medidas de seguridad con el objetivo de proteger un mismo activo. Es una táctica que utiliza varias capas, en la que cada una provee un nivel de protección adicional a las demás.



Figura 6. El enfoque en capas nos permitirá organizar mejor los controles que implementemos y aumentar la seguridad de nuestra organización.

Como veremos más adelante en este capítulo, ninguna medida de seguridad puede ser perfecta, por lo que es mucho mejor contar con varias medidas, cada una de las cuales cumplirá su papel. Esto hace que no tengamos una dependencia absoluta de una sola medida de seguridad, lo que nos permite la posibilidad de fallo y genera que sea mucho más complejo acceder a un sistema de forma no autorizada. Esta estrategia ha sido formulada por la **NSA** (*National Security Agency*) como un enfoque para la seguridad informática y electrónica.

Figura 7. La **NSA** (www.nsa.gov) es la agencia criptológica del gobierno de los Estados Unidos. Es un excelente recurso de información, ya que constantemente se publican documentos de interés.



En un principio, este concepto se utilizó como una estrategia militar que buscaba retrasar más que prevenir el avance del enemigo, lo que permitía ganar tiempo, muy valioso en el campo de batalla.

Debemos implementar las medidas basándonos en el paradigma de **proteger, detectar y reaccionar**. Esto significa que, además de incorporar mecanismos de protección, tenemos que estar preparados para recibir ataques e implementar métodos de detección y procedimientos que nos permitan reaccionar y recuperarnos de dichos ataques.

Es muy importante balancear el foco de las contramedidas en los tres elementos primarios de una organización: personas, tecnología y operaciones.

- **Personas:** alcanzar un nivel de seguridad óptimo empieza con el compromiso de la alta gerencia, basado en un claro entendimiento de las amenazas. Este debe ser seguido por la creación de políticas y procedimientos, la estipulación de roles y responsabilidades, la asignación

de recursos y la capacitación de los empleados. Además, es necesario implementar medidas de seguridad física y control de personal con el fin de monitorizar las instalaciones críticas para la organización.

- **Tecnología:** para asegurar que las tecnologías implementadas son las correctas, deben establecerse políticas y procedimientos para la adquisición de la tecnología. Es preciso implementar varios mecanismos de seguridad entre las amenazas y sus objetivos; cada uno debe incluir sistemas de protección y detección.
- **Operaciones:** se enfocan en las actividades necesarias para sostener la seguridad de la organización en las tareas cotidianas. Este tipo de medidas incluye: mantener una clara política de seguridad, documentar todos los cambios efectuados en la infraestructura, realizar análisis de seguridad periódicos e implementar métodos de recuperación.

El principio KISS

El **principio KISS** recomienda la implementación de partes sencillas, comprensibles y con errores de fácil detección y corrección, rechazando lo complicado e innecesario en el desarrollo de una solución.

El origen de este acrónimo es la frase en inglés *Keep It Simple, Stupid* (que, traducido al español, significa: “manténlo simple, estúpido”). Para ser menos ofensivos, podríamos decir *Keep It Simple & Secure* (“manténlo simple y seguro”).



MULTIPLICAR MEDIDAS



Desde el punto de vista del atacante, es mucho más difícil penetrar un sistema que cuente con varias medidas de seguridad, debido a que siempre existe la posibilidad de que una de ellas sea fácilmente saltada, aprovechando un error humano o alguna otra condición particular. Si hay varias medidas y una es saltada, habrá otras para proteger el sistema.



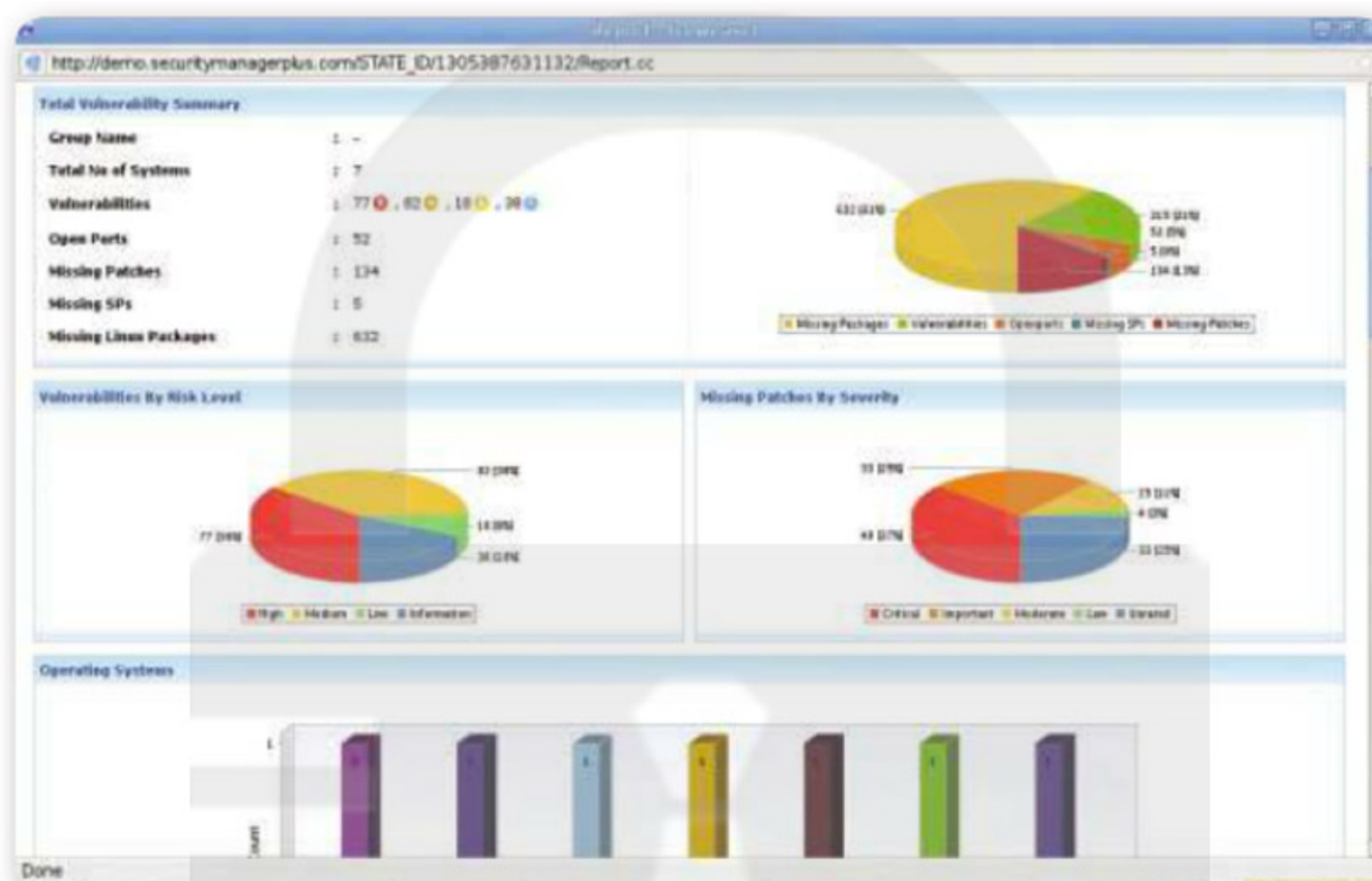


Figura 8. Muchas herramientas buscan mostrar de forma simple y gráfica el estado de la seguridad. Esto permite entender rápidamente cuál es la situación actual para, luego, enfocarnos en los detalles.

La idea detrás de esto corresponde a la certeza de que las cosas simples y fáciles de entender suelen tener mejor aceptación que las cosas complejas. Además, son mucho más fáciles de mantener, y esto es muy importante para las soluciones de seguridad, que muchas veces suelen caer en una excesiva complejidad, lo que termina en soluciones inentendibles y difíciles de sostener.

Este concepto está relacionado directamente con el **principio de parsimonia**, según el cual, “cuando dos teorías en igualdad de condiciones tienen las mismas consecuencias, la más simple tiene más probabilidades de ser correcta que la compleja”. Este principio es atribuido a Guillermo de Ockham, por lo que también es conocido como **navaja de Ockham**. Este precepto puede (y debe) ser aplicado siempre y cuando nos encontremos en la situación de tener que elegir entre varios controles de seguridad que sean iguales o muy semejantes en cuanto a los beneficios que pueden aportarnos pero diferentes en cuanto a su diseño y complejidad.

Debemos prestar mucha atención a esto y no caer en implementar lo que nos sea más fácil aun a costa de minimizar la funcionalidad o perder el foco de nuestro objetivo. Por lo tanto, es fundamental hacer un análisis completo de las soluciones disponibles, teniendo en cuenta que, a veces, la complejidad de una solución es la única forma de que esta satisfaga verdaderamente nuestras necesidades.

También hay que considerar los recursos con los que contamos para implementar un control de seguridad, tanto humanos, como de tiempo y dinero. Esto será fundamental para la toma de decisiones, debido a que una solución compleja, a la larga, puede ser imposible de mantener por una organización pequeña, en tanto que una demasiado sencilla puede no ser suficiente para los requerimientos de una organización grande.

Desde arriba hacia abajo

Cuando se construye un edificio, el proyecto empieza con el diseño de los planos; luego, se construye la base y el resto del edificio, con cada puerta y ventana en su lugar, como está especificado en los planos. A continuación, los inspectores verifican que el edificio esté bien construido y que siga las indicaciones de los planos. ¿Notaron la cantidad de veces que aparece la palabra “planos”? ¡Es porque son muy importantes! Los **objetivos** de una organización son los planos de un edificio. Deben estar bien



USB INHABILITADO



Para proteger los puertos USB que no se utilizaban, una empresa decidió introducir pegamento en ellos para bloquearlos físicamente. Varios meses después, descubrieron que los nuevos teclados, mouse y tokens de seguridad requerían una conexión USB. Quitar el pegamento e implementar una herramienta para el control de puertos representó un gasto de tiempo y dinero que se podría haber evitado.



definidos desde el principio para que todo el programa de seguridad esté desarrollado en base a ellos.

Muchas veces, las organizaciones toman el camino corto y empiezan a instalar aplicaciones de seguridad y a poner pegamento en los puertos USB para bloquearlos (sí, algunos hacen eso realmente). El problema no está en lo precario de aplicar el pegamento sino en lo inútil de trabajar sin saber a dónde queremos llegar.

Lo que debemos hacer es empezar por una idea amplia y poco específica de lo que queremos obtener. Luego, sobre la base de estas ideas, pasaremos a trabajar en los detalles de las tareas que vamos a realizar para alcanzar los objetivos fijados.

El siguiente paso es desarrollar e implementar las guías, estándares y procedimientos que van a soportar las ideas generales escritas inicialmente. A medida que avanzamos en el proceso, vamos siendo cada vez más específicos, pero siempre con los objetivos principales en mente, hasta llegar a definir cada una de las configuraciones necesarias para cumplir con nuestras metas.



Figura 9. Una vez que tenemos los objetivos definidos, desarrollamos la táctica para alcanzarlos. Hecho esto, estaremos en condiciones de pensar en las técnicas que utilizaremos.

Es importante trabajar con esta metodología porque eso hace que no necesitemos realizar cambios drásticos ni rediseñar grandes partes de nuestros planes. Al principio, puede parecer que este enfoque lleva más tiempo y trabajo pero, a medida que avancemos, notaremos que es el enfoque más sencillo, práctico y acertado.

Un programa de seguridad debe estar soportado y dirigido por la alta gerencia para luego ser distribuido hacia abajo en el árbol jerárquico, hasta alcanzar a toda la organización. Este enfoque se conoce como **desde arriba hacia abajo**. De esta forma, es fácil que toda la organización sea contagiada con los conceptos propuestos y se logre un trabajo armonioso y cooperativo. Este es el enfoque indicado si consideramos que la seguridad de la información debe ser prioridad dentro de los objetivos de la organización, que son definidos, como cualquier otro, por la alta gerencia.



La seguridad en las empresas

Las empresas, de forma consciente o inconsciente, han volcado sus procesos de negocio a los sistemas de información. Con el fin de volverse más productivas, ahorrar costos y poder realizar negocios en todas partes del mundo, las empresas han transformado cada una de sus operaciones en parte de una aplicación informática. La información, que años atrás era almacenada en papel (que podía guardarse en un lugar conocido, leerse, copiarse y



ELECCIÓN DE HERRAMIENTAS



Existen varias herramientas de seguridad que pueden permitirnos reducir los tiempos que nos lleva realizar ciertas tareas. Debemos tener en cuenta sus capacidades técnicas y los beneficios que pueden traernos en nuestro trabajo. Además de aumentar la seguridad de nuestros sistemas, también sirven para ahorrar recursos, tanto de tiempo como de dinero.



destruirse a mano), ahora se encuentra dispersa en forma de ceros y unos, dentro de varios medios de almacenamiento, como memorias USB, discos duros, dispositivos ópticos, y otros. Esto ha creado una amplia diversidad de fuentes de información, que nosotros estamos encargados de proteger.



Figura 10. Los pendrives USB han abierto nuevas formas de ataque, debido a que son un excelente hogar para todo tipo de virus. Además, son un medio muy utilizado para el robo de información.

Dentro de las filas de una organización que se rige por un presupuesto, nuestros recursos para brindar protección y seguridad serán limitados. Algunas empresas asignan más capital a la seguridad informática que otras, pero lo cierto es que todos, en mayor o menor medida, nos encontramos limitados en cuanto a los recursos de que podemos disponer para realizar nuestras tareas. Como buenos profesionales de la seguridad, debemos tener en cuenta las necesidades de la organización, con el fin de alinear las prácticas de seguridad con los objetivos de la empresa. Esto es imprescindible si pretendemos integrar la seguridad como uno de los procesos de negocio.

La seguridad como proceso de negocio

Como vimos anteriormente, el compromiso con la seguridad debe partir desde lo más alto del árbol jerárquico de una organización:

la alta gerencia. Para esto, es necesario que las personas encargadas de definir los rumbos de la empresa vean la seguridad como un proceso que no los obliga a gastar dinero, sino que les permite tanto ahorrarlo como ganarlo. Básicamente, si aseguramos los sistemas de modo que no haya interrupciones de servicio, estaremos ahorrando el dinero que perderíamos al no poder trabajar. Si les demostramos a nuestros clientes un compromiso con la seguridad de sus datos y con brindar un servicio de primer nivel, estaremos ganando más dinero porque atraeremos más clientes y mantendremos contentos a los que ya tenemos. Estos son, simplemente, dos ejemplos de cómo podemos utilizar la seguridad informática con objetivos directamente relacionados con el negocio.

Para todo profesional de la seguridad, es de suma importancia tener la capacidad de exponer estos conceptos ante los directivos de una empresa, con el objetivo de llamar su atención. Como cada persona habla su propio lenguaje, dependiendo de su área de especialización, es imposible que podamos convencer al gerente de marketing sobre las ventajas del nuevo sistema de protección de datos personales, si le marcamos que lo bueno del sistema es que está programado en Python y que usa una capa de abstracción que permite extender el sistema por medio de plugins que se desarrollan utilizando la API del fabricante. Seguramente, apenas escuche la palabra “Python” dejará de prestarnos atención.

Una situación muy distinta puede darse si le explicamos que tener un sistema de protección de datos personales permite asegurar a nuestros



RECURSOS



Debemos recordar que, cuando hablamos de recursos, no tenemos que considerar solamente el dinero: también debemos tener en cuenta los recursos humanos y los tiempos de los que disponemos, los cuales, muchas veces, terminan siendo factores tanto o más importantes que los recursos monetarios.



clientes que sus datos se encuentran protegidos por una tecnología muy avanzada que garantiza que nuestra organización cuidará de ellos y de sus intereses. Siempre debemos hablar en el lenguaje de nuestro interlocutor; esta es una de nuestras tareas como verdaderos profesionales.

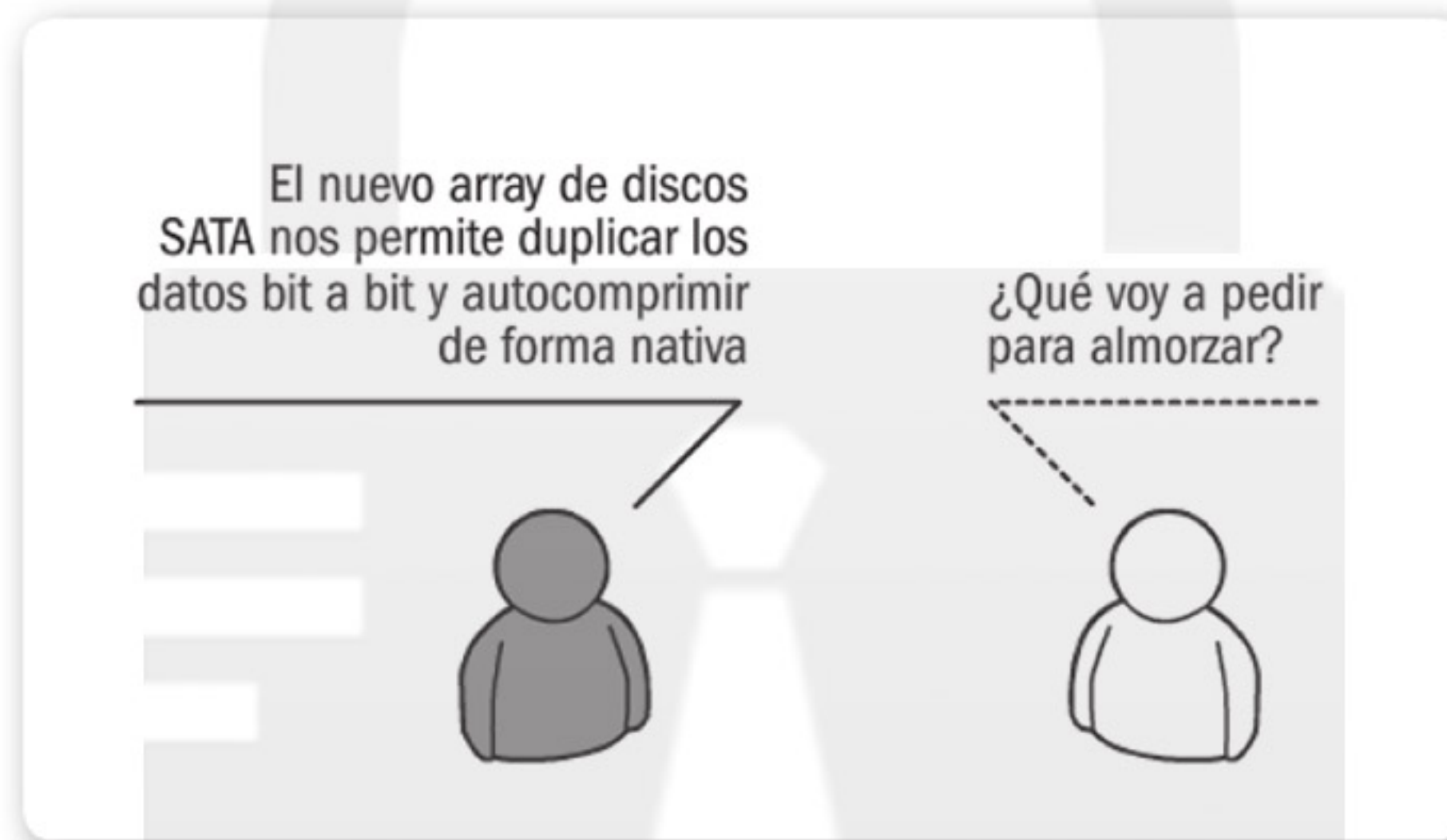


Figura 11. Tengamos en cuenta con quién estamos hablando y pensemos correctamente en qué decir y cómo hacerlo. De lo contrario, es muy probable que no nos presten la atención que deseamos.

Es una excelente idea que, antes de hablar con personas ajenas al ámbito de la seguridad informática, tengamos unos minutos para reflexionar acerca de qué ventajas debemos exponer. Ponernos en la piel de la otra



PROBAR CONTINUAMENTE



Es recomendable probar nuevos productos aunque no vayamos a utilizarlos. Así conoceremos las herramientas y las nuevas capacidades que ofrecen. Ya sea para analizar futuras compras o para implementar esas funcionalidades nosotros mismos, estar al tanto de las últimas tendencias es un requisito para mantenernos como profesionales de elite.

persona y analizar sus necesidades nos permitirá conectarnos mejor con cada uno de los integrantes de la empresa.

Recordando estos consejos podremos lograr que la seguridad informática sea vista en toda la organización como algo necesario, que no se hace por obligación sino por una necesidad, ya que mantener la empresa segura beneficia a todos.



Métricas de seguridad

No podemos hablar de seguridad si no tenemos la capacidad de medir de alguna manera su estado, por eso es necesario contar con una metodología que nos ayude a comprender en detalle nuestra situación actual y pasada. Siendo más específicos, es necesario que, por lo menos, podamos contestar a la pregunta básica: ¿cuánto hemos mejorado nuestra seguridad con respecto al año anterior? El verdadero objetivo de hacernos esta pregunta es contar con una respuesta que pueda ser entregada a la alta gerencia con el objetivo de asistirle en la toma de decisiones que marcarán el rumbo de la organización. Por lo tanto, las métricas que definimos y los valores que obtenemos tienen que poder ser expresados en un lenguaje entendible desde el punto de vista del negocio. Podemos tener grandes reportes con datos y vulnerabilidades identificadas, pero estos carecerán de sentido si no sabemos qué queremos responder y cómo esto beneficia a la organización.

Lo cierto es que necesitaremos, al menos, dos tipos de métricas. La primera debe tener un enfoque técnico y nos servirá para analizar en qué puntos podemos mejorar, qué vulnerabilidades debemos atacar primero, qué medidas de seguridad están teniendo éxito, cuáles deben ser reemplazadas o modificadas, etcétera. Este reporte estará destinado a las áreas tecnológicas y debe ser revisado por personal idóneo, que tenga la capacidad de proponer mejoras y adquirir nuevas soluciones.

El segundo reporte debe ser dirigido a la dirección de la empresa y su objetivo es mostrar un pantallazo general acerca de cuál es la situación



con respecto a la seguridad: en qué hemos mejorado, en qué debemos mejorar y si existen nuevas problemáticas que necesitemos resolver. También podemos incluir propuestas de inversión, ya sea de recursos tecnológicos, recursos humanos o capacitaciones al personal.

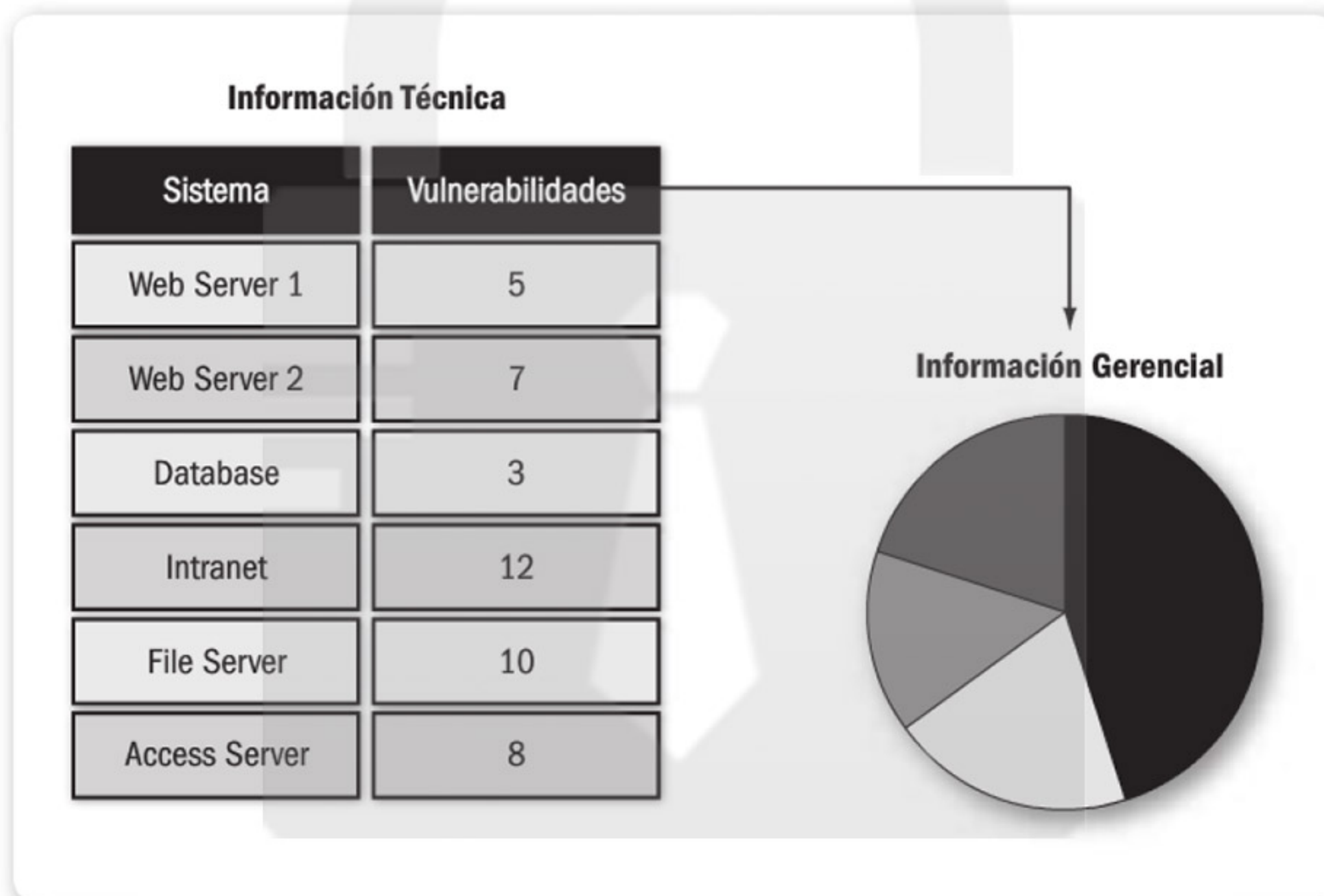


Figura 12. Sobre la base de la información técnica, generalmente obtenida de varias herramientas, debemos generar reportes sencillos, enfocados en la gerencia.

También debemos tener en cuenta que no todo es medible, porque existen valores subjetivos de los que no podremos obtener gráficos ni valores concretos. Por ejemplo, en el caso de que nuestro sitio web sea atacado y modificado, la pérdida de credibilidad que sufrirá nuestra organización no será medible (aunque sin duda será algo muy negativo).

Para resumir la importancia de las métricas, debemos recordar una frase que se aplica no solo a la seguridad, sino también a la gestión de cualquier proceso: “Si no lo puedes medir, no lo podrás gestionar”.



Mejora continua

El proceso de **mejora continua** es un concepto que pretende mejorar los productos, servicios y procesos en todos los niveles de una compañía. Al igual que los conceptos anteriores, este debe ser implementado como actitud constante por cualquier organización que desee alcanzar objetivos ambiciosos. Formalmente, los sistemas de gestión de calidad, las normas ISO y los sistemas de evaluación ambiental se utilizan para alcanzar objetivos relacionados con la mejora continua. Más allá de esto, no es necesario seguir estrictamente estas guías para entrar en un ciclo de mejoramiento permanente, pero son excelentes puntos de partida.

En general, es posible conseguir una mejora continua reduciendo la complejidad y los puntos potenciales de fracaso; mejorando la comunicación, la automatización y las herramientas, y colocando puntos de control y salvaguardas para proteger la calidad de las operaciones de una organización.

Más allá de que existen documentos y normativas relacionados con el proceso de mejora continua, debemos tomar este concepto por lo que es (un concepto) y aceptar que cualquier metodología que nos lleve a un proceso de mejora continua será necesaria y debe ser bienvenida por la organización. Para esto, hay que seleccionar las metodologías que mejor se adapten a las necesidades particulares de cada entorno.

Debemos saber también que, así como no es posible alcanzar la perfección, tampoco es posible lograr un ambiente 100% seguro. Simplemente, esto es algo a lo que podemos aspirar a través de varios esfuerzos bien dirigidos. Pero cabe recordar que este es un trabajo constante, que nunca llega a un final porque siempre está persiguiendo una perfección que no se deja alcanzar. Visto de otro modo: la perfección siempre intenta alejarse de nosotros. Depende de nuestras capacidades el hecho de que podamos seguirle el paso y mantenernos siempre pisándole los talones.

Es imperativo que tengamos la capacidad de mantener los procesos de nuestra organización al nivel más simplificado posible (KISS) y que seamos capaces de medir los resultados dentro de una línea de tiempo (métricas).



Haciendo esto, tendremos las herramientas necesarias para mejorar la calidad de nuestros procesos constantemente (mejora continua).

La seguridad absoluta es algo imposible. Tendremos que aprender a vivir con eso. Una vez que hayamos asimilado esta idea, podremos empezar a pensar en acercarnos a la perfección, sabiendo que nunca lograremos alcanzarla. El trabajo arduo y constante nos llevará a perfeccionarnos, a mejorar nuestras capacidades de respuesta y a predecir los eventos que podrían causar un impacto negativo en nuestras organizaciones.

Esto es un entrenamiento que va más allá de un curso o de un título de grado: se consigue con la experiencia cotidiana y con la capacidad de mirar hacia atrás para no volver a cometer los errores pasados y aventurarnos a cometer errores nuevos. Siempre depende de nosotros ser excelentes profesionales.



RESUMEN



En este capítulo conocimos las características y metodologías de trabajo de un profesional de la seguridad informática. Analizamos la seguridad como proceso de negocio, cómo involucrar a las distintas áreas de una empresa y la importancia de las métricas y la mejora continua para poder ofrecer un buen servicio.

Actividades

TEST DE AUTOEVALUACIÓN

- 1 ¿Cuáles son las ventajas y desventajas de la superespecialización?
- 2 ¿A qué hace referencia el principio KISS?
- 3 ¿Cuáles son las ventajas de implementar defensa en profundidad?
- 4 ¿Es posible lograr que una organización sea 100% segura? ¿Por qué?
- 5 ¿Por qué son importantes las métricas de seguridad?



PROFESOR EN LÍNEA



Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: **profesor@redusers.com**

Gestión de la seguridad

En este capítulo comprenderemos el proceso de gestión de la seguridad informática, entenderemos las responsabilidades que tiene cada persona dentro de la organización y veremos cómo y por qué deben redactarse los documentos formales. Además, analizaremos cómo identificar las amenazas, vulnerabilidades y riesgos con los que nos enfrentamos.

▼ Introducción.....	36	▼ Políticas y otros documentos	52
▼ El autoconocimiento.....	37	▼ Responsabilidades.....	57
▼ Amenazas y vulnerabilidades.....	43	▼ Resumen.....	63
▼ Implementación de controles.....	49	▼ Actividades.....	64



Introducción

La gestión de la seguridad es un proceso amplio, que incluye muchísimas tareas de distinta índole, como la administración de riesgos, el mantenimiento de políticas, la clasificación de la información y la capacitación de los miembros de la organización.

Por eso nos encontramos con una profesión tan apasionante, que demanda de nosotros una gran variedad de conocimientos. Dentro de ella, podremos encontrar varias especializaciones, cada una de las cuales puede tener un foco más técnico o más administrativo, pero que comparten los mismos fundamentos, que debemos conocer a la perfección si queremos garantizar la elección e implementación correcta de las medidas de seguridad. La única diferencia que debe existir entre unos y otros profesionales es el porcentaje de contacto que tendrán con cada uno de los aspectos de la seguridad.

Dado que un gerente pasará más horas de su jornada redactando y analizando políticas, y que un administrador analizará configuraciones de sistemas y redes durante la mayor parte de su tiempo, ambos deben conocer en su totalidad las tareas por realizar.

Una metodología que puede sernos de gran interés es **OCTAVE**, publicada por el **CERT Coordination Center**, de la **Universidad de Carnegie Mellon**. Se trata de una metodología mucho más extensa, que cuenta con una versión para pequeñas y medianas empresas, conocida como **OCTAVE-S**.



ANÁLISIS DE SEGURIDAD



Para ser excelentes profesionales, debemos tener la capacidad de analizar todo el proceso de gestión de la seguridad, conociendo todas las tareas que se realizan, aunque sea de una manera superficial. Solo así podremos tener una visión global, que nos permitirá optimizar nuestras actividades para alcanzar los objetivos de la organización.





Figura 1. En el sitio web del **CERT** (www.cert.org) además de la metodología **OCTAVE**, podemos encontrar una gran cantidad de información y documentos de interés.

En el sitio web en inglés <http://sisainfosec.com/blog/comparison-between-iso-27005-octave-nist-sp-800-30-2> encontramos un completo informe que compara las características de **SP 800-30** y **OCTAVE**, y que además integra las ventajas de **ISO 27005**.

El autoconocimiento

La importancia de conocernos a nosotros mismos y saber exactamente a qué debemos temer, es la clave para tener éxito, no solo en la seguridad informática. Para remarcar la importancia de este tema, citaremos un fragmento del milenario libro *El arte de la guerra*, de **Sun Tzu**:

“Si conoces al enemigo y te conoces a ti mismo, no te pondrán en peligro ni cien batallas. Si no conoces al enemigo, pero te conoces a ti mismo, perderás una y ganarás otra. Si no te conoces ni a ti ni al enemigo, estarás en peligro en todas las batallas”.

Como podemos observar, conocernos a nosotros mismos y conocer los peligros que rondan a nuestro alrededor es de vital importancia para obtener la victoria en la tarea de asegurar nuestra información.

Es por eso que, antes de pensar siquiera en implementar medidas de seguridad, debemos tomar acciones para conocer a fondo nuestra infraestructura tecnológica. De este modo, podremos asignarles un valor a los activos que la componen y, así, definir nuestras prioridades y los recursos que vamos a invertir para proteger cada uno de ellos.

Recordemos que la tecnología no es otra cosa que una herramienta que simplifica tareas y optimiza procesos. Por eso, el conocimiento de qué sistemas son importantes para la organización está ligado estrechamente a los procesos de negocio, los cuales están a cargo de los directivos y gerentes.

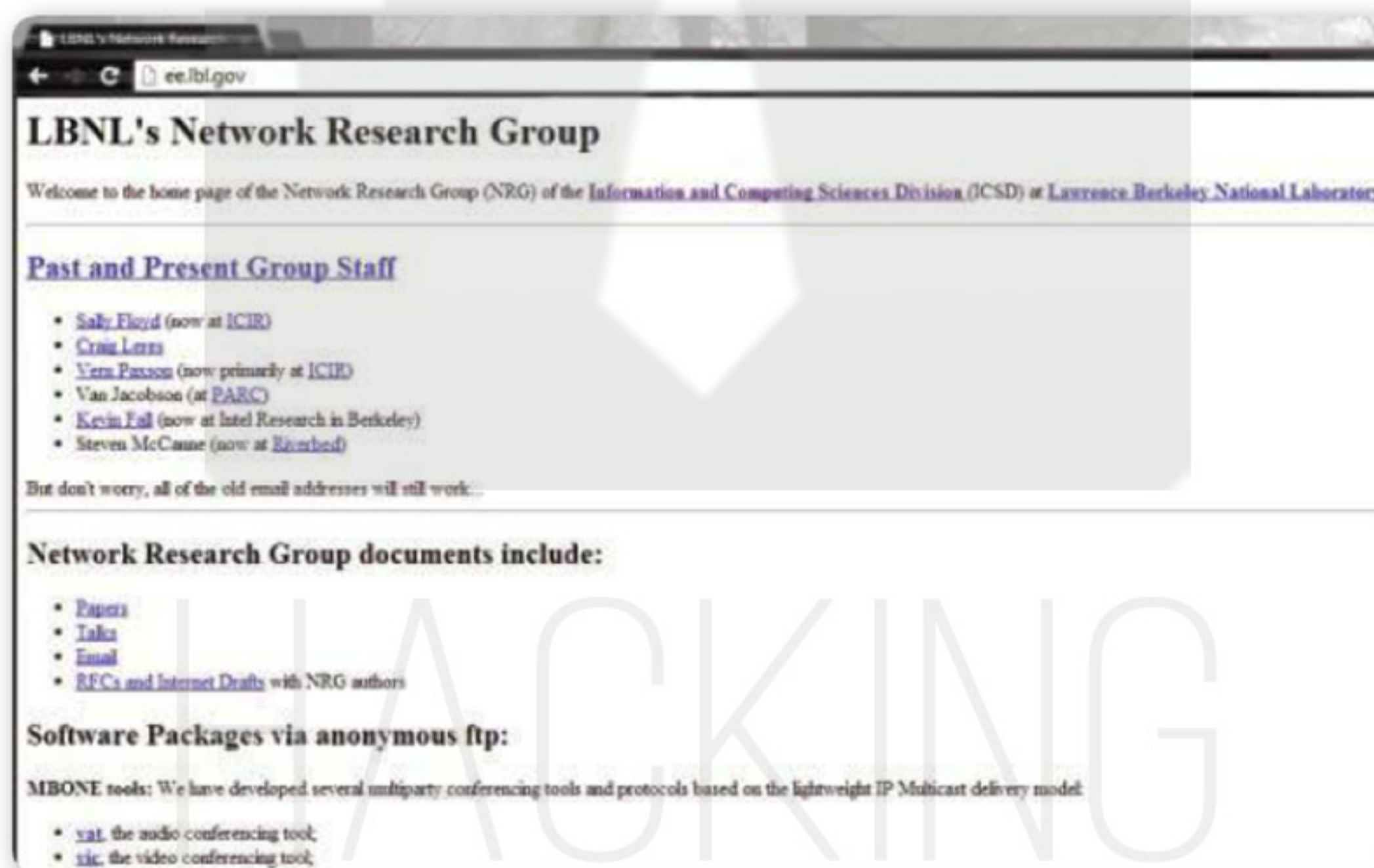


Figura 2. Arpwatch (<http://ee.lbl.gov>) es un software de código abierto que nos permite conocer los cambios de direcciones en los dispositivos de nuestra red. Es ideal para estar al tanto de nuevos equipos.

Así que para determinar cuáles son los sistemas más importantes, tendremos que consultar a los altos mandos de la organización. Por supuesto,

como analizamos anteriormente, las consultas a los directivos deben realizarse teniendo en cuenta el lenguaje de nuestro interlocutor, por lo que tendremos que realizarlas en una forma parecida a la siguiente:

- ¿Cuáles son las funciones principales del negocio?
- ¿Cuáles son las tareas más importantes dentro de la organización?
- ¿Qué tareas no pueden interrumpirse?
- ¿Qué tareas pueden ser interrumpidas durante muy poco tiempo?
- ¿Qué espera de su infraestructura tecnológica?

Esto nos da una idea del tipo de preguntas que debemos realizar, ya sea a través de cuestionarios o de entrevistas personales. Con las respuestas que obtengamos, podremos verificar qué sistemas intervienen en cada uno de estos procesos y, así, determinar la criticidad que tiene cada activo para la organización.



Figura 3. OCS Inventory (www.ocsinventory-ng.org/en) es un software de código abierto que nos permite mantener actualizado un inventario de software y hardware.

Una vez que tengamos bien identificados los procesos de negocio críticos, debemos pasar a describir nuestra infraestructura tecnológica. Para esto, podemos entrevistarnos con los encargados de las áreas técnicas, que la mantienen, personalmente o con cuestionarios, y analizando la documentación existente. Los datos acerca de la infraestructura serán:

- Usuarios (tanto los que brindan soporte como los que la utilizan).
- Topología de la red actual (diagramas de red).
- Flujo de información (conexiones con otros sistemas, internos y externos).
- Tareas del sector de IT (copias de seguridad, mantenimiento, replicación de datos, procedimientos para alta, baja y modificación de cuentas, etcétera).

Para cada uno de los dispositivos registrados debemos tomar nota de:

- El propósito que cumple.
- Hardware y software.
- Configuraciones.
- Información que almacena y/o procesa.
- Personas que lo utilizan.

Es de vital importancia poder conectar las respuestas obtenidas de la gerencia con el inventario de activos de información, para determinar qué



CLASIFICAR ACTIVOS



Muchas empresas pasan por alto la tarea de clasificar sus activos, pensando que ya conocen su infraestructura por el hecho de estar en contacto con ella constantemente. Este es un error muy común, pero grave. El primer paso, y requisito fundamental para la seguridad informática, es conocer exactamente qué tenemos y cuánto vale para nosotros.

sistemas intervienen en el desarrollo de cada uno de los procesos de negocio identificados como críticos.



Figura 4. Netdisco (www.netdisco.org) es un software de código abierto que mantiene un inventario de los dispositivos de red existentes. Puede detectar nuevos dispositivos a través de **SNMP**, **CDP** y **LLDP**.

Con todos estos datos a nuestra disposición, estaremos en condiciones de armar una tabla de activos y prioridades, la cual vamos a necesitar para completar las siguientes etapas del proceso de gestión.

Análisis cualitativo vs. cuantitativo

Al clasificar cada activo de la organización, nuestro principal objetivo será asignarle un valor, que refleje la importancia que tiene para nosotros. Para esto, existen dos tipos de análisis: el cuantitativo, en el que asignamos valores monetarios a cada uno de nuestros activos; y el cualitativo, en el cual nos basamos en valores de una escala (por ejemplo, de 1 a 10) para reflejar la importancia que le otorgamos a cada uno.

Cada método tiene sus ventajas y desventajas. Podemos destacar, rápidamente, que los análisis cuantitativos son más exactos y más fáciles de entender por la gerencia, pero requieren un trabajo muchísimo mayor y una gran cantidad de cálculos. Por su parte, los cualitativos se basan más en la percepción de necesidad que tienen las personas sobre un activo, lo que los vuelve mucho más sencillos de realizar y, si bien pueden ser no tan exactos, conforman una excelente fuente de información para la toma de decisiones.

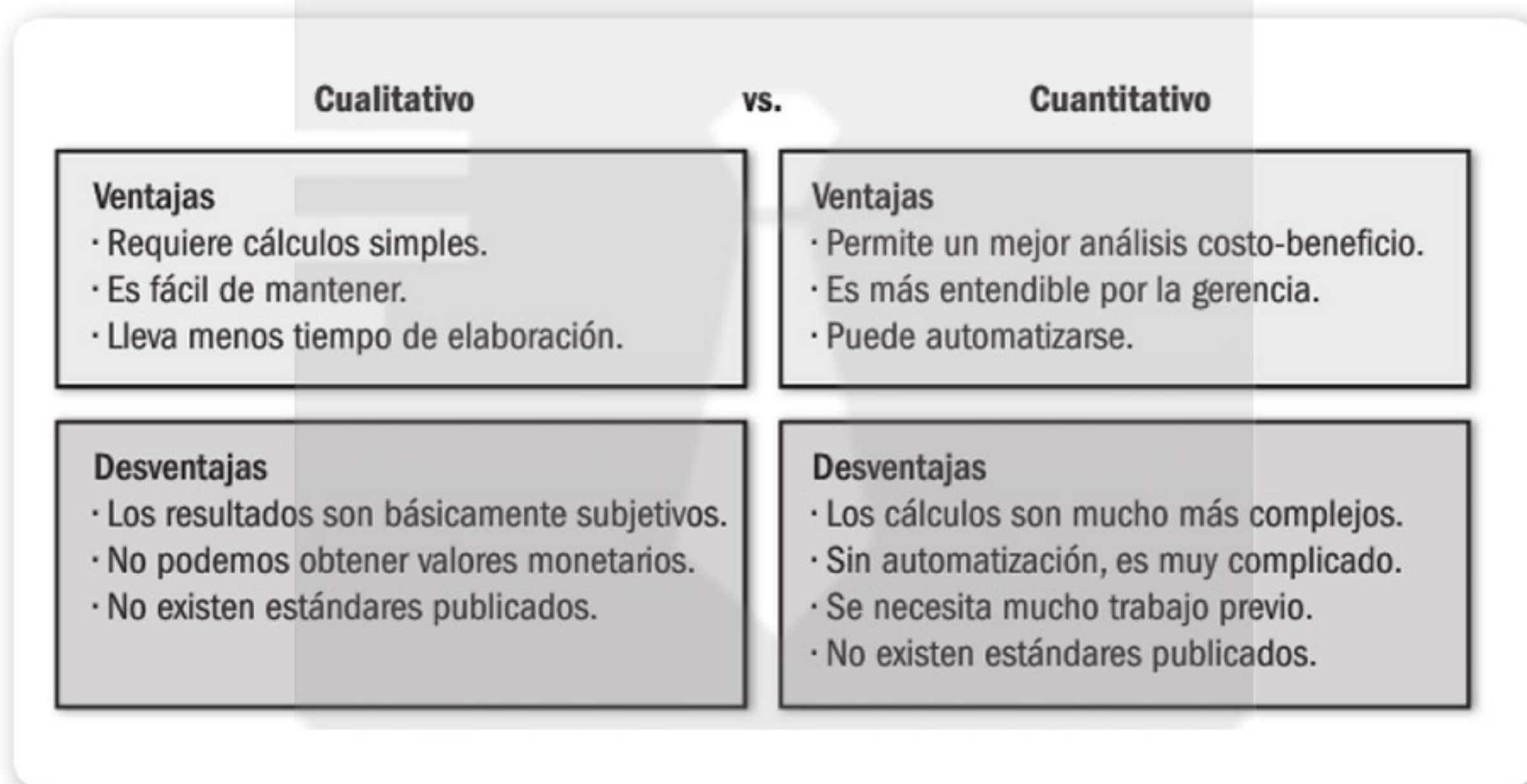


Figura 5. En el diagrama analizamos brevemente las ventajas y desventajas de cada uno de los sistemas de valoración.

El tipo de análisis que vayamos a utilizar dependerá de cada uno de nosotros, según nuestros recursos y necesidades. En la mayoría de los casos, bastará con un análisis cualitativo, que nos permitirá conocer los valores de nuestros activos para poder asignarles prioridades.

Como expertos en seguridad, sacaremos más provecho a la lista ordenada de mayor a menor de los activos más importantes, que al valor de estos en sí. Dicha lista nos permitirá analizar sobre qué activos debemos trabajar primero y asignarles más recursos.

Tanto en los análisis cualitativos como en los cuantitativos, podemos utilizar los conceptos de la Tríada CID analizada anteriormente, al asignar la importancia de un activo, y darle a cada uno valores separados para **Confidencialidad**, **Integridad** y **Disponibilidad**. Hacerlo nos permitirá obtener valores mucho más exactos cuando tengamos que analizar posibles pérdidas, pero también tornará el análisis mucho más complejo, ya que habrá que obtener tres valores por cada activo analizado. Esto es algo que, generalmente, no es necesario, y suele recomendarse que se deje para un análisis posterior. Pero, como siempre, la elección dependerá de cada organización.



Amenazas y vulnerabilidades

Cuando hablamos de gestión de la seguridad, es muy frecuente el uso de ciertos términos que, a veces, se intercambian incorrectamente y suelen prestarse a confusión. Aquí analizaremos con brevedad cada uno de ellos, tomando como ejemplo la situación de contar con una estación de trabajo que no tiene un antivirus instalado.

Vulnerabilidad: es una debilidad en algún software, hardware o procedimiento que puede permitir a un atacante realizar acciones que, normalmente, no tiene permitidas. En general, tiene como raíz la ausencia o



ANÁLISIS CUALITATIVO



Es importante considerar que en las organizaciones que se inician en el proceso de gestión de la seguridad, es recomendable utilizar un análisis cualitativo y asignar un único valor a la importancia de cada activo que se encuentre presente. Una vez hecho esto, tenemos la opción de volvernos más minuciosos y pasar a un análisis cuantitativo o asignar un valor para cada concepto de la Tríada CID.

la debilidad en uno o más controles. En nuestro ejemplo, la vulnerabilidad es la ausencia de antivirus.

Amenaza: es cualquier peligro potencial sobre la información y/o los sistemas. La amenaza es alguien o algo que aprovecha una vulnerabilidad existente y la utiliza para provocar un daño. Puede ser de tipo no intencional (como errores humanos, tornados, terremotos) o intencional (hackers, empleados furiosos, etcétera). En nuestro ejemplo, la amenaza es el virus.

Exposición: se refiere al impacto negativo que podríamos llegar a sufrir en caso de que la vulnerabilidad fuera explotada. El término exposición hace referencia al daño probable. Cuando este daño se vuelve real, se lo conoce como impacto. En nuestro ejemplo, estamos expuestos a que la estación se infecte y suframos la pérdida y/o corrupción de datos, además de su mal funcionamiento.



Figura 6. En la imagen podemos ver en acción la herramienta antimalware **TrendMicro**, la cual es implementada como una medida de protección contra virus y otros tipos de malware.

Riesgo: es el resultado de analizar la vulnerabilidad, la amenaza, la exposición y la probabilidad de explotación. En nuestro ejemplo, el riesgo es la probabilidad de que el virus infecte a la estación de trabajo. Suele categorizarse en bajo, medio o alto.

Contramedida: se utiliza para mitigar los riesgos. Puede ser una configuración de software, un dispositivo o un procedimiento que elimine la vulnerabilidad o reduzca el riesgo de ocurrencia de que un agente de ataque explote dicha vulnerabilidad. En nuestro ejemplo, la contramedida podría ser instalar un antivirus, acción que mitigaría el riesgo de una infección de virus.



Figura 7. Proceso detallado acerca de cómo una vulnerabilidad puede causar problemas y cómo debemos mitigarla a través de contramedidas.

Una vulnerabilidad puede ser explotada por una amenaza, hecho que generaría un cierto grado de exposición. Esto representa un riesgo, que es mitigable a través de contramedidas.

Citando el ejemplo: “La ausencia de un antivirus en una estación de trabajo podría ser explotada por un virus, lo cual la expone a ser infectada y perder sus datos. Esto representa un alto riesgo para ella, que puede ser mitigado instalando un antivirus”.

Aclarados estos términos, nuestra siguiente tarea es identificar cuáles son las amenazas que podrían impactar sobre nuestros activos. Debemos

considerar tanto amenazas físicas como lógicas, y tanto intencionales como accidentales. Algunas de las más comunes son los hackers, los empleados descontentos y la competencia.

Para esto, podemos desarrollar una tabla con las amenazas más probables, a fin de contar con un listado que nos permita tener una buena visión acerca de cuáles son los peligros a los que nos enfrentamos. Es fundamental armar esta tabla con todas las amenazas que se nos ocurran, para, luego, ir descartando las que sean muy poco probables o no se apliquen a nuestro entorno. Una vez que tengamos identificadas las principales amenazas, podemos empezar a trabajar sobre ellas, dejando las otras para siguientes repeticiones del proceso. Lo importante es poner manos a la obra y empezar el trabajo; luego, con el tiempo, iremos mejorando sobre la marcha y a partir de la experiencia.

	Intencionales	No intencionales
Lógicas	• Hackers • Malware • Empleados descontentos	• Fallas de sistema • Empleados (errores de uso)
Físicas	• Ataques terroristas • Empleados descontentos	• Inundaciones • Terremotos • Fallas de hardware

Figura 8. En la imagen vemos una tabla con las posibles amenazas a las cuales se enfrenta una organización. Dependerá de cada situación particular si algunas de ellas se aplican o no, pero esta lista sirve para tener una idea de cómo confeccionar nuestra propia tabla.

Una vez que hayamos completado la tabla de amenazas, procederemos a investigar qué vulnerabilidades tenemos en nuestros sistemas. Ya sea a través del análisis minucioso de las configuraciones, el uso de herramientas automa-

tizadas o cualquier otro método, obtendremos una lista de cada uno de los activos, con las vulnerabilidades que presenta. Es necesario emplear varios métodos para recabar este tipo de información, como analizar configuraciones, leer manuales y utilizar herramientas automatizadas, pero debemos saber que es necesario unificar estos datos, para trabajarlos de manera adecuada.

Activo	Vulnerabilidad	Amenaza probable
Estaciones de trabajo	• Fallas de antivirus • Puertos USB sin restricciones • Usuario Guest habilitado	• Malware • Usuarios descontentos • Hackers
Servidores	• Firewall deshabilitado • Sistema operativo desactualizado • Sin copias de respaldo de los datos	• Hackers • Malware • Usuarios descontentos - Falla de hardware
Router externo	• Telnet habilitado • Falta de redundancia de hardware • ACL no definidas	• Hackers • Falta de hardware

Figura 9. En la imagen vemos un listado de vulnerabilidades conocidas por activo, y las amenazas que podrían aprovecharlas para causar daños.



ERRORES NO INTENCIONALES



Tanto por experiencia profesional como a partir del resultado de varias estadísticas, podemos observar que una gran parte de los incidentes de seguridad son iniciados a través de accidentes, fallas o acciones no intencionales. Estos errores son muy comunes, sobre todo, por parte de usuarios inexpertos o en entornos en los que se realizan tareas muy complejas.

Para poder hacer uso de toda la información recolectada, deberemos ordenarla con el fin de poder realizar comparaciones y filtrados. Esto puede lograrse a través de herramientas especializadas, la creación de alguna pequeña herramienta con una base de datos relacional o haciendo un uso exhaustivo de planillas de cálculo.

Lo importante de contar con una tabla de activos con vulnerabilidades explotables es que nos garantiza la capacidad de asignarles prioridad a aquellos que corren más peligro. Utilizaremos esta tabla en el siguiente paso.



Figura 10. Este proyecto de código abierto está basado en el código de **Nessus** e intenta llenar el vacío que este dejó cuando pasó a ser totalmente software privativo (www.openvas.org).

Como final del proceso de identificación, obtendremos una tabla con los niveles de riesgo que tiene cada activo, sobre la base de cada una de las vulnerabilidades que posee. Con esto, podremos identificar rápidamente a qué acciones dar prioridad y recursos cuanto antes. Este tipo de tablas requiere una buena cantidad de cálculos matemáticos (sobre todo, cuando disponemos de muchos activos). Es por eso que es ampliamente recomendable automatizar el proceso de algún modo.



Activo	Valor	Vulnerabilidad	Amenazas	Exposición	Probabilidad	Riesgo	Total Vuln
Servidor de archivos	5	Sin copias de seguridad	· Falla de hardware	5	3	75	145
			· Empleados (error de uso)	2	3	30	
			· Empleados descontentos	2	2	20	
Servidor de correo	5	· Software desactualizado · Sin copias de seguridad	· Hackers	4	3	60	60
			· Falla de hardware	5	3	75	75
Estaciones de trabajo	3	· Sin antivirus · Sin copias de seguridad	· Malware	4	5	60	60
			· Falla de hardware	5	2	30	30
Impresoras y escáneres	1	Admin sin password	· Usuarios descontentos	4	2	8	8

Escala de valores: Muy alta (5), Alta (4), Media (3), Baja (2) y Muy baja (1).

Figura 11. En la tabla podemos ver que la mayor necesidad es la de implementar un sistema de copias de seguridad para el servidor de archivos, que también podríamos utilizar para el servidor de correo.



Implementación de controles

Una vez que tenemos identificados los riesgos, debemos hacer algo con ellos. En caso contrario, todo el esfuerzo realizado hasta el momento será en vano. No podemos, simplemente, barrer los riesgos debajo de la alfombra y hacer como si nada de esto hubiera sucedido.

Así que tenemos que elegir cómo vamos a reaccionar ante cada uno de los riesgos y, para eso, necesitamos hacer un análisis de costo/beneficio a fin de determinar cuál será la mejor manera de actuar en cada caso. Podemos optar entre cuatro posibilidades, que son:

Mitigar: implementar medidas para reducir o eliminar un riesgo. Por ejemplo, para reducir el riesgo de una infección por virus, podemos instalar un software antivirus.

Transferir: para transferir un riesgo a otra organización, generalmente podemos contratar un seguro para el activo que queremos proteger. Por ejemplo, para transferir el riesgo de que un dispositivo sufra una falla de hardware, podemos extender su garantía, y así asegurarnos un reemplazo de partes. Obviamente, esto no nos protege de una pérdida de información o de caídas de servicio, por lo cual debemos tener mucho cuidado al analizar qué riesgo estamos transfiriendo.

Evadir: cuando hablamos de evadir un riesgo, estamos haciendo referencia a eliminar la fuente que lo produce. Esto quiere decir que preferimos dejar de utilizar un activo o proceso con tal de no sufrir los riesgos asociados a él. Por ejemplo, para evadir los riesgos que conlleva el uso de software de mensajería instantánea, podemos optar por bloquear su implementación.

Aceptar: este es el último recurso y debe ser utilizado solo cuando no podamos optar por ninguna otra alternativa. Cuando hablamos de aceptar un riesgo, estamos diciendo que tendremos que convivir con él, porque no resulta rentable implementar medidas de seguridad, pero de todos modos



RECOMENDADOS



Algunas de las herramientas gratuitas que podemos utilizar para automatizar la búsqueda de vulnerabilidades son: **OpenVAS** (www.openvas.org); **Nexpose Community Edition**, de los mismos creadores de **Metasploit Framework** (www.rapid7.com); y **Microsoft Baseline Security Analyzer**, que sirve solo para plataformas **Microsoft**, (<http://technet.microsoft.com/es-cl/security/cc184924.aspx>).



necesitamos la fuente que lo produce. Debemos tratar de mantener los riesgos aceptados en la menor cantidad posible.

	Mitigar	Evadir	Transferir	Aceptar
Ventajas	• Permite un buen balance entre seguridad y funcionalidad. • Nos permite tener un mejor control. • Es la solución más personalizable. • Es la solución mejor vista en las auditorías.	• Suele ser una opción económica. • Puede ser de rápida implementación.	• Permite resolver rápido un problema.	• Es la opción más económica.
Desventajas	• Puede requerir investigación y adquisición de soluciones. • Puede tardar bastante tiempo en implementarse.	• No siempre es aplicable. • Podría hacernos perder funcionalidad.	• No siempre podemos hacerlo. • Puede tener un costo muy elevado.	• Al final, puede ser la más costosa. • En cierta forma, nos estamos dando por vencidos. • No siempre podemos hacerlo. • No es bien visto en las auditorías.

Figura 12. La tabla muestra una comparativa de las cuatro opciones que tenemos para lidiar con los riesgos, destacando las principales ventajas y desventajas de cada una.



PRÁCTICA PROFESIONAL



Cuando aceptamos un riesgo, esto implica que alguien debe hacerse responsable de esa decisión y de las consecuencias que pueda llegar a traer haberlo aceptado. Es por eso que se deben considerar cuidadosamente las otras tres alternativas, antes de aceptar un riesgo. Si, a pesar de todo, se decide enfrentarlo, es ampliamente recomendable exigir la firma de un documento por parte de la gerencia para cada caso específico.

De todas estas opciones, siempre debemos tener en mente la mitigación como primera medida. Y solo cuando esta sea impracticable o ineficiente, deberemos considerar alguna de las otras. Recordemos que los riesgos van a estar ahí, aun cuando intentemos mirar hacia otro lado, así que es mucho mejor hacerles frente de manera temprana, antes que después sufrir las consecuencias de no haberles dado la importancia que se merecían.



Políticas y otros documentos

Como analizamos en el **Capítulo 1**, es necesario contar con un enfoque que va desde arriba hacia abajo, empezando por la alta dirección y bajando por todos los niveles jerárquicos. Este enfoque será menos específico en los niveles más altos, y aumentará su complejidad y sofisticación a medida que vayamos descendiendo.

Es preciso tener en cuenta que la seguridad de una organización va muchísimo más allá de una regla en un firewall o de la configuración de un sistema de prevención de intrusos. Incluso, si bien estas son cuestiones que afectan a la seguridad, terminan siendo el resultado de un análisis que se inicia al escribir los documentos que servirán como guía para este tipo de tareas.

A continuación, analizaremos los distintos tipos de documentos con los que debemos contar, y daremos recomendaciones al elaborar cada uno de ellos.

Políticas

Son los documentos que explican las bases sobre las cuales la organización realiza sus tareas y busca cumplir sus objetivos. No tratan ningún tema en profundidad; al contrario, son una referencia a la misión y la visión a través de las cuales debe guiarse cada uno de los miembros.

Tienen que estar escritas o, por lo menos, avaladas por la alta gerencia, debido a que explican la postura de la organización con respecto a la se-



guridad, y están basadas en los objetivos del negocio. También se deben tener presentes las leyes, los estándares y las reglamentaciones a los cuales la organización debe atenerse.

Cada vez que la organización es modificada de alguna manera significativa, dichas políticas deben ser revisadas y cambiadas de forma acorde. También deben ser periódicamente revisadas para realizar las optimizaciones o correcciones correspondientes. Por eso, debemos escribirlas de manera generalizada, con el objetivo de no tener que modificarlas constantemente.

Es recomendable que estos documentos estén redactados en forma sencilla y fácilmente entendible, para ser usados como punto de referencia por cualquier empleado de la organización. Es preciso remarcar la importancia que tienen y aclarar siempre las obligaciones de cada uno de los empleados, utilizando el modo imperativo (términos como “tiene/debe” en vez de “tendría/debería”).

Cada uno de los empleados debe saber que esta política explica lo que la organización espera de ellos. Por consiguiente, la violación a los conceptos que dicha política plantea, podría (y debería) implicar la aplicación de sanciones.

Si bien pueden existir varias políticas que cubran aspectos específicos, la principal y más general suele ser llamada “política de seguridad de la información”. Otras podrían estar destinadas a temas como: “uso de internet y correo electrónico”, “información confidencial”, etcétera.



POLÍTICAS



Si esperamos que los empleados de una organización sigan al pie de la letra lo que dicta la política de seguridad, es necesario que hagamos accesible este documento a todos ellos, para que tengan la posibilidad de consultarlo cuando lo crean oportuno. También es muy recomendable que cada miembro de la organización acepte formalmente esta política.

Como las políticas deben escribirse desde un punto de vista global, es necesaria la independencia de cualquier tecnología o producto específico.



Figura 13. En el sitio del **SANS Institute** encontramos guías que harán más fácil la redacción de documentos (www.sans.org/security-resources/policies).

Estándares

Estos documentos explican en qué forma van a ser alcanzados los objetivos propuestos por la organización en cuanto a aspectos de seguridad.



NORMATIVAS Y ESTÁNDARES PROBADOS



Es una buena idea tomar las bases de normativas, estándares y recomendaciones ya avalados por entidades reconocidas para formular nuestros documentos. Esto nos permitirá disponer de contenido ampliamente revisado y desarrollado por expertos en la materia. Luego, podremos adaptarlos a las necesidades particulares de nuestra organización.



Dictan de qué manera deben ser encarados los problemas y cómo tomar las decisiones.

Muchas veces, suelen ser documentos generados por entidades externas y que son tomados por las organizaciones, ya sea en parte o en su totalidad.



Figura 14. En el sitio web del **Center for Internet Security** encontraremos, entre otras cosas, estándares recomendados para la configuración de nuestros sistemas operativos y dispositivos de redes (www.cisecurity.org).

En estos documentos podemos empezar a hablar de tecnologías específicas (algoritmos de encriptación, sistemas operativos, arquitecturas de hardware, etcétera). Pero debemos hacerlo de un modo general, sin adentrarnos en el nombramiento de versiones específicas ni en otros detalles que dejaremos para los siguientes documentos.

Con los estándares vamos a reflejar las tácticas de la organización, que estarán derivadas de la estrategia (lo que reflejan las políticas).

Es importante que prestemos mucha atención al redactar un estándar o tomar uno externo, debido a que necesitaremos verificar que este se encuentre alineado con la política y que sea una buena base para la redacción de los procedimientos.

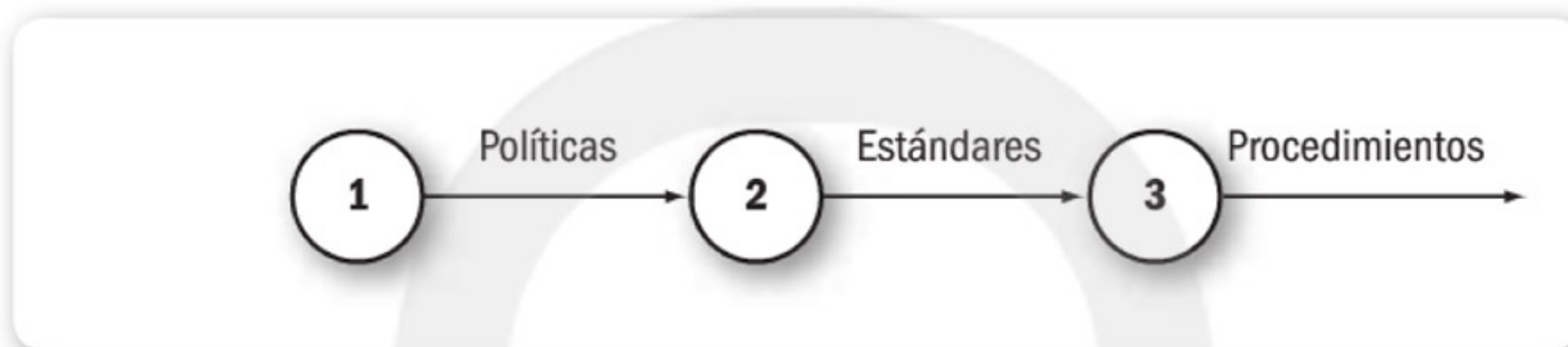


Figura 15. Debemos respetar el orden en el cual generamos los documentos que guiarán nuestras tareas. Es un proceso lineal, donde cada documento se basa y nutre de los contenidos del anterior.

Procedimientos

Derivan de los estándares, y son los documentos que se encuentran en el nivel más práctico de todos. Esto significa que van a ser bien detallados, como guías paso a paso, que expliquen cómo realizar las tareas.

UN PROCEDIMIENTO
DEBE ENTREGAR
DETALLES PARA
REALIZAR UNA TAREA
ESPECÍFICA



Son los documentos que más se modifican, debido a que la tecnología suele cambiar, y las nuevas versiones de los productos que utilizamos seguramente se instalarán y administrarán de manera diferente de sus predecesoras.

En este caso debemos ser lo más específicos posible, y pensar que un procedimiento debería permitir que una persona que no contara con una vasta experiencia realizara la tarea mencionada sin mayores inconvenientes. Esto también nos servirá de gran ayuda cuando necesitemos hacer un reemplazo, debido a la partida de un integrante, o a una ausencia, ya sea por vacaciones, enfermedad o cualquier otro motivo.

La tarea de mantener actualizados los procedimientos debe ser constante, y tenemos que asegurarnos de marcar bien cuál es la última versión del documento, debido a que, en muchas ocasiones, puede ocurrir que existan varias versiones, lo que genera muchísima confusión.



Políticas • Basadas en la visión y misión de la empresa. • Redactadas o avaladas por la alta gerencia. • Independientes de cualquier tecnología o producto.	Estándares • Reflejan las tácticas de la organización. • Hablan de tecnologías, pero no de productos. • Pueden estar basados en estándares externos.	Procedimientos • Datallan paso a paso cómo se realizan las tareas. • Son específicos en cuanto a productos y versiones. • Deben ser actualizados con frecuencia.
--	---	---

Figura 16. La tabla muestra las principales características de cada uno de los distintos documentos aquí mencionados.

Tanto para los procedimientos, como para los estándares y las políticas, consideremos utilizar un repositorio conocido por todos los miembros de la organización, que esté bien ordenado y nos permita realizar controles de acceso. Esto nos dará la posibilidad de optimizar las tareas de mantenimiento, evitará confusiones y garantizará un mejor seguimiento con el correr del tiempo.

Además, muchos procedimientos podrían llegar a contener información que no es recomendable que sea conocida por todos los integrantes de la organización. Por lo tanto, un repositorio o servidor de archivos nos permitirá definir permisos granulares, con el objetivo de restringir el acceso de los empleados únicamente a los documentos que precisan para realizar sus tareas correctamente.



Responsabilidades

La seguridad informática tiene mucho que ver con las responsabilidades, debido a que nuestra tarea es proteger. A veces nos olvidamos de esto porque todo marcha bien, pero sin duda lo recordaremos cuando haya algún problema y alguien tenga que responder por eso. Una de nuestras principales tareas es no solo ser responsables de nuestros actos, sino también recordarles a los demás que también tienen responsabilidades que cumplir.

Después de todo, no podemos pretender que una persona actúe de forma responsable si desconoce cuáles son sus responsabilidades y las actitudes que la organización espera de ella.

Desde la alta gerencia, hasta los empleados de más bajo rango, todos los integrantes de la organización tienen distintas obligaciones que cumplir y, también, son responsables de velar por los intereses comunes. Esto debe ser puesto en claro desde un primer momento, para evitar confusiones y malos entendidos que más tarde pueden ser catastróficos, tanto para la empresa como para las personas que la componen.

En última instancia, la responsabilidad de cada una de las acciones que lleva a cabo una organización recae sobre sus directores. Es por eso que debemos tener en cuenta que, más allá de los premios y castigos que puede recibir un empleado, la mayoría de las veces quienes tienen que responder ante la ley son los directores.

El equipo de seguridad

Para lograr una implementación correcta de las medidas de seguridad, es necesario que cada organización cuente con un equipo designado a mantenerlas.

Dependiendo del tamaño de cada entidad, de sus capacidades económicas y sus políticas de seguridad, el equipo puede estar conformado por una (algo bastante solitario y decepcionante) o varias personas.



DUE DILIGENCE



El término **due diligence** es el acto de investigar y entender los riesgos con los cuales se enfrenta una organización. Por su parte, **due care** implica que la organización demuestra un compromiso con la seguridad, implementando medidas, redactando documentos y generando conciencia en los empleados. Estos dos términos son muy importantes.



El objetivo de este equipo es coordinar y mantener las políticas, estándares, procedimientos y medidas de seguridad aplicadas, así como también realizar periódicamente revisiones y auditorías, y aconsejar a la alta gerencia.

Además, este equipo debe contar con colaboradores designados de cada una de las principales áreas de la organización. Como tarea de tiempo parcial, ellos intervendrán en la asistencia a reuniones periódicas, el reporte de estado, y otros aspectos. El objetivo último de este equipo es garantizar que las medidas de seguridad se implementen de manera efectiva.

Si analizamos algunas de las normativas y las formas de procedimiento de las empresas más grandes de los Estados Unidos y varios países de Europa, veremos que existen no uno, sino varios equipos relacionados con la seguridad informática, como pueden ser el de gestión de riesgos, el de seguridad informática y el de respuesta a incidentes, entre otros.

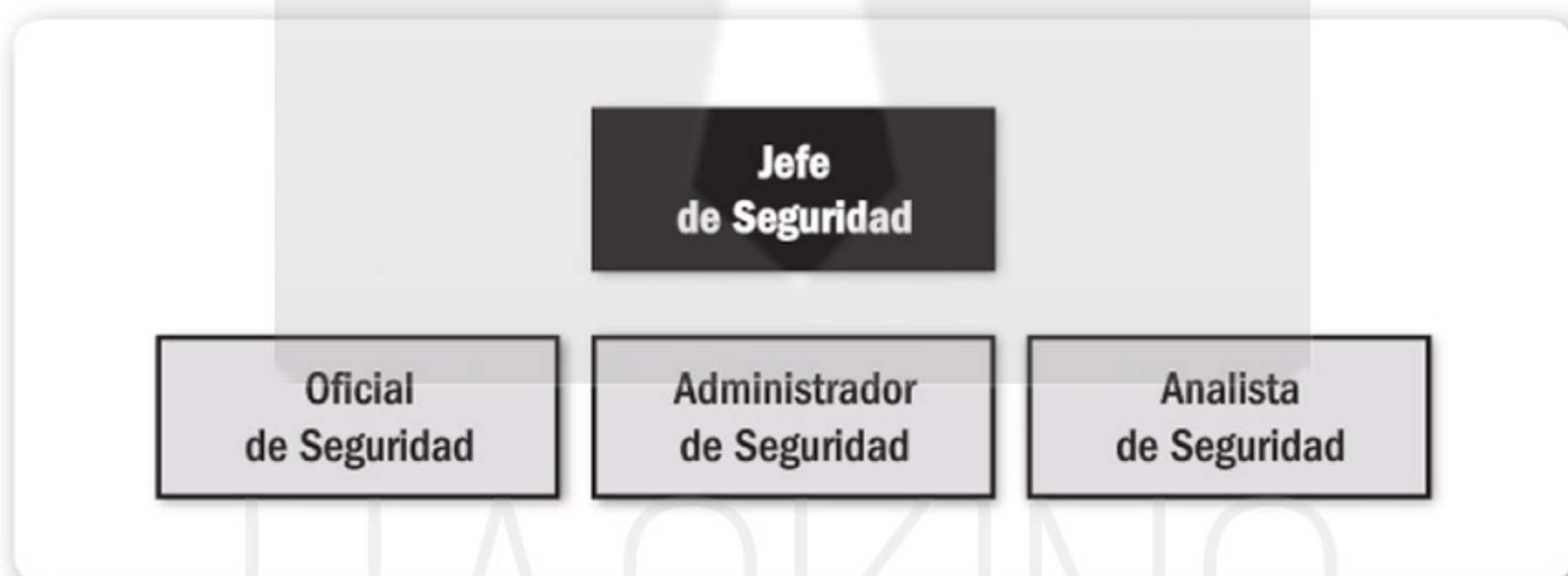


Figura 17. Algunas normativas exigen una determinada estructura básica para los equipos de seguridad, como la que podemos ver en la figura.

Dentro de ella, existen distintos roles para la separación de tareas.

Esto es algo que no todas las empresas pueden permitirse y, principalmente, que no todas las empresas necesitan. Es por eso que tenemos que analizar cuáles son nuestras verdaderas necesidades y crear equipos sobre esa base, teniendo en cuenta que una cantidad excesiva de equipos nos traerá problemas de coordinación y burocracias innecesarias.



Figura 18. El sitio web de **Inteco** (www.inteco.es) es un excelente recurso de información para que nuestro equipo de seguridad se mantenga actualizado.

La mayoría de las empresas puede cumplir todos sus requerimientos con un equipo dedicado exclusivamente a la seguridad informática y con colaboradores de cada uno de los departamentos. También debemos asegurarnos de que dicho equipo reciba capacitaciones constantes, y cuente con los recursos imprescindibles para llevar a cabo sus tareas y mantenerse al tanto de lo que pasa en el mundo de la tecnología.

Capacitación al personal

Es bien sabido que el personal técnico y relacionado con la seguridad informática debe recibir un entrenamiento constante, para estar actualizado en cuanto a las últimas medidas de seguridad y las nuevas tendencias. Pero no siempre se tiene en cuenta que la seguridad informática es un tema que abarca a las organizaciones en su totalidad, y es por eso que cada uno de sus miembros debe tener las nociones y los fundamentos de seguridad bien presentes.

Muchas de las vulnerabilidades e incidentes de seguridad ocurren por negligencia de los usuarios. Pero esto no quiere decir que la culpa sea de los propios usuarios, sino más bien de los responsables de la organización, que no vieron la importancia de capacitarlos correctamente. Es por eso que debemos tener en cuenta la necesidad de desarrollar un programa de capacitaciones dirigido específicamente a los usuarios finales, para educarlos y que sepan exactamente cómo comportarse y reaccionar ante cualquier actividad sospechosa.

La forma más efectiva de brindar estas capacitaciones es ponerlas a disposición de los usuarios de manera online, y luego, hacer que ellos tengan que rendir un pequeño examen, de preguntas al azar, para demostrar que han prestado atención al contenido visto, y estar seguros de que lo han entendido. También es bueno enviar noticias y consejos de seguridad periódicamente, no tanto con la esperanza de que los empleados los sigan al pie de la letra, sino para que nos tengan presentes en todo momento y sepan que estamos para ayudarlos.

Dueños, custodios y usuarios de datos

Si bien la información en su totalidad pertenece a la organización, es necesario que, para protegerla correctamente, sean asignados los roles de dueños y custodios. Esto es así porque tiene que existir alguien que dicte



RECURSOS HUMANOS



El Departamento de Recursos Humanos es el nexo entre los miembros de la organización y la organización en sí misma. Como interviene en los procesos de contratación, modificación de roles y despido, es imprescindible que se mantenga un contacto fluido entre este departamento y el equipo de seguridad informática. De ellos depende que este equipo esté al tanto de las cosas antes de que sucedan, para poder tomar las acciones correspondientes en tiempo y forma.

las formas en las cuales se van a proteger los datos, y que se haga responsable por lo que se hace con ellos.

En general, es una buena idea definir a los dueños de datos basándonos en el departamento al cual pertenece dicha información. Por ejemplo, para los datos relacionados con el marketing, podemos señalar rápidamente al Gerente de Marketing como dueño. Esto hace que dicha persona tenga ciertas obligaciones y derechos por sobre esa información, que deben ser impuestos por la alta gerencia. Así serán respetados al pie de la letra y quedará clara la importancia de este tipo de responsabilidades.

La persona que tenga el rol de dueño de datos estará encargada de comunicar al equipo de seguridad informática cómo debe ser protegida la información, y de explicar qué importancia tiene esta para la organización y las tareas que su departamento realiza. Además, podrá definir qué usuarios accederán a dichos datos y con qué permisos.

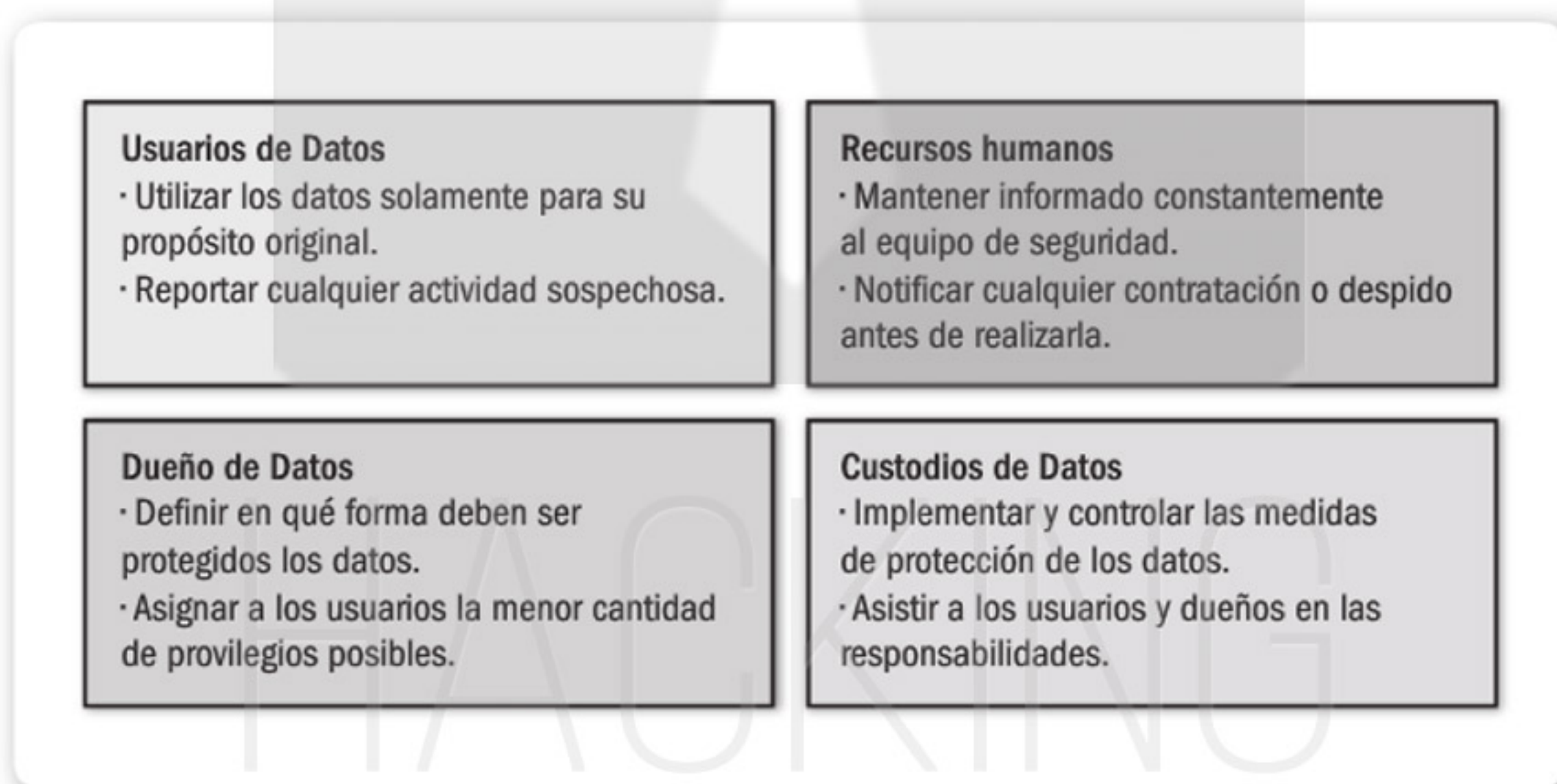


Figura 19. En el gráfico podemos ver las responsabilidades más importantes de cada uno de los roles. Debemos tener en cuenta que absolutamente todos los integrantes son usuarios de datos, aun cuando tengan otros roles adicionales.

Los custodios de datos serán miembros del equipo de seguridad informática. Estarán encargados de asegurar que la información sea tra-

tada y protegida de acuerdo con lo solicitado por sus dueños. También verificarán que los controles funcionen correctamente y que no se violen las políticas de seguridad definidas. Además, se ocuparán del mantenimiento de los permisos asignados a los usuarios, eliminando los que corresponda cuando alguien deja la organización, y verificando que se quiten los que ya son innecesarios cuando alguien cambia de sector o se modifica su rol en la empresa.

Por otra parte, los usuarios también tienen una responsabilidad muy importante, que es la de utilizar los datos en forma correcta y sin malas intenciones, cumpliendo con lo que dictan las políticas de seguridad, sin difundir datos confidenciales ni realizar ninguna acción que pudiera perjudicar de alguna manera a la empresa. También tienen la responsabilidad de denunciar cualquier comportamiento sospechoso que pueda tener alguno de sus compañeros.

El hecho de que todos y cada uno de los miembros de la organización cumplan correctamente con sus responsabilidades es una de las bases más importantes para poder garantizar la protección de la información.



RESUMEN



En este capítulo efectuamos una completa introducción al proceso de gestión de seguridad, vimos la importancia del autoconocimiento y de tener en cuenta a qué situaciones debemos temer para lograr una mejor seguridad informática. Vimos las características de un análisis cualitativo y de un análisis cuantitativo, y conocimos las amenazas y vulnerabilidades más importantes. Finalmente, revisamos la implementación de controles y definimos las políticas y estándares.

Actividades

TEST DE AUTOEVALUACIÓN

- 1 ¿Cuáles son las ventajas y desventajas del análisis cualitativo?
- 2 ¿Cómo se relaciona el nivel de riesgo con las amenazas y las vulnerabilidades?
- 3 ¿Cuáles son las cuatro formas de responder ante un riesgo identificado?
- 4 ¿Qué diferencias existen entre una política, un estándar y un procedimiento?
- 5 ¿Cuáles son las responsabilidades de los dueños y custodios de datos?



PROFESOR EN LÍNEA



Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: **profesor@redusers.com**



Continuidad del negocio

Mediante los conceptos expuestos en este capítulo aprenderemos a seleccionar qué datos se deben respaldar y revisaremos la forma adecuada de efectuarlo. También veremos cómo mantener el control de nuestra infraestructura a través del monitoreo y nos prepararemos para responder correctamente ante los eventos adversos.

▼ Introducción.....	66	▼ Gestión de incidentes.....	78
▼ Copias de respaldo	67	▼ BIA, BCP y DRP	81
▼ Monitoreo.....	71	▼ Resumen.....	89
▼ Control de cambios.....	74	▼ Actividades.....	90



Introducción

Hasta ahora hemos analizado las tareas que debemos llevar a cabo para prevenir o minimizar las probabilidades de que nuestros sistemas sufran algún impacto negativo, estudiando los riesgos y teniéndolos bajo control. Con estos cuidados, ya tenemos la mitad de la batalla ganada. ¿Cuál es la otra mitad? Saber qué debemos hacer cuando las cosas malas suceden.

Parte de ser excelentes profesionales recae en nuestra capacidad de estar al tanto de la completa situación de nuestra infraestructura y hasta de poder conocer eventos futuros. Así estaremos completamente preparados y responderemos de la mejor manera posible.

A esto se lo conoce como **continuidad del negocio**, e implica tener la capacidad de hacer resistente una organización: resistente a los eventos adversos y a aquellas situaciones que, de no estar preparados, la harían desaparecer. Esto no es poca cosa y, así como es difícil garantizar la subsistencia financiera de una empresa, es difícil garantizar la subsistencia de los sistemas. Pero ahí se encuentra gran parte de la diversión de nuestro trabajo: en la incertidumbre y los riesgos a los cuales tenemos que hacer frente.

Deberemos tener en cuenta una gran cantidad de variables para poder realizar un planeamiento correcto. Este es un proyecto largo y complejo, que nos consumirá un tiempo considerable; claro que, si lo hacemos bien,

los resultados serán más que satisfactorios, y el nivel de seguridad de nuestra organización aumentará notablemente.

En las siguientes páginas analizaremos cómo debemos realizar el planeamiento y la redacción de documentos correspondientes a la continuidad del negocio de nuestra organización. Cada uno de estos pasos nos será de vital importancia, tanto en los momentos de trabajo diario como en los de crisis, durante los cuales debemos saber exactamente qué hacer y cómo lograrlo.

LA CONTINUIDAD DEL
NEGOCIO HACE QUE
LA ORGANIZACIÓN
RESISTA EVENTOS
ADVERSOS





Copias de respaldo

Una copia de seguridad es como contratar un seguro médico: esperamos nunca tener que usarlo, pero si lo necesitamos, tiene que responder a la perfección. Realizar esta tarea es fundamental porque, según la Cámara de Comercio de Londres, el 90% de las empresas que sufren una pérdida de datos importante desaparece del mercado en dos años.

Sin embargo, como no es habitual tener la necesidad de restaurar una copia de seguridad, las empresas suelen restarle importancia al proceso de realizarlas. Al ser encargados de la seguridad, esta es una de nuestras tareas: hacer que todos los datos de valor para la organización sean respaldados regularmente, y que estos respaldos sean probados en intervalos de tiempo determinados.

Principalmente, debemos basarnos en el testimonio de los dueños de datos a la hora de definir cada cuánto realizar los backups y por cuánto tiempo almacenarlos. Además, habrá que tener en cuenta las disposiciones legales y regulatorias, que muchas veces exigen determinados criterios de almacenamiento. Si no tenemos definidos los dueños de datos, tendremos que utilizar el resultado de la clasificación de activos. Y si no hicimos la clasificación de activos, podremos usar nuestra intuición.

Bacula es una herramienta para realizar copias de seguridad. Es de código abierto y multiplataforma. Funciona con la arquitectura cliente/servidor y nos permite instalar agentes en cada uno de los equipos que queremos respaldar, configurando varias opciones.



HERRAMIENTAS RECOMENDADAS



Algunas de las herramientas de código abierto que pueden simplificar el proceso de realizar y mantener copias de seguridad son Bacula (www.bacula.org), Amanda (www.amanda.org) y BackupPC (<http://backuppc.sourceforge.net>). También existen otras propietarias, como Acronis (www.acronis.com) y Arkeia (www.arkeia.com).



Figura 1. Para obtener más información sobre **Bacula**, podemos entrar a su sitio web: **www.bacula.org**.

La selección del lugar en donde vamos a almacenar las copias de seguridad dependerá de qué eventos adversos esperamos que puedan suceder. Si queremos contemplar la posibilidad de un incendio o una inundación en nuestro centro de datos, no sería nada inteligente almacenar las copias en ese mismo sitio.

Por lo general, suele ser suficiente elegir un lugar que esté en el mismo edificio, pero lejos del centro de datos, y protegido por una caja fuerte a prueba de calor. En otros casos, nos encontraremos ante



COPIAS DE SEGURIDAD

Es preciso tener en cuenta que las copias de seguridad deben ser cuidadas como un activo más de información. Suelen contener datos confidenciales, por lo que siempre es recomendable encriptarlas. Además, deben ser fácilmente identificables para que el encargado de restaurar los datos pierda el menor tiempo posible en buscar la copia correcta.



la necesidad de almacenarlos fuera del edificio, ya sea en un centro de datos alternativo o en alguna otra ubicación.

Además, es necesario que verifiquemos periódicamente el funcionamiento de los métodos de recuperación. No hace falta probar cada una de las copias, pero sí tenemos que seleccionar una al azar para hacerlo. Eso nos dará la seguridad tanto de que los datos están ahí, como de que las herramientas empleadas funcionan correctamente.

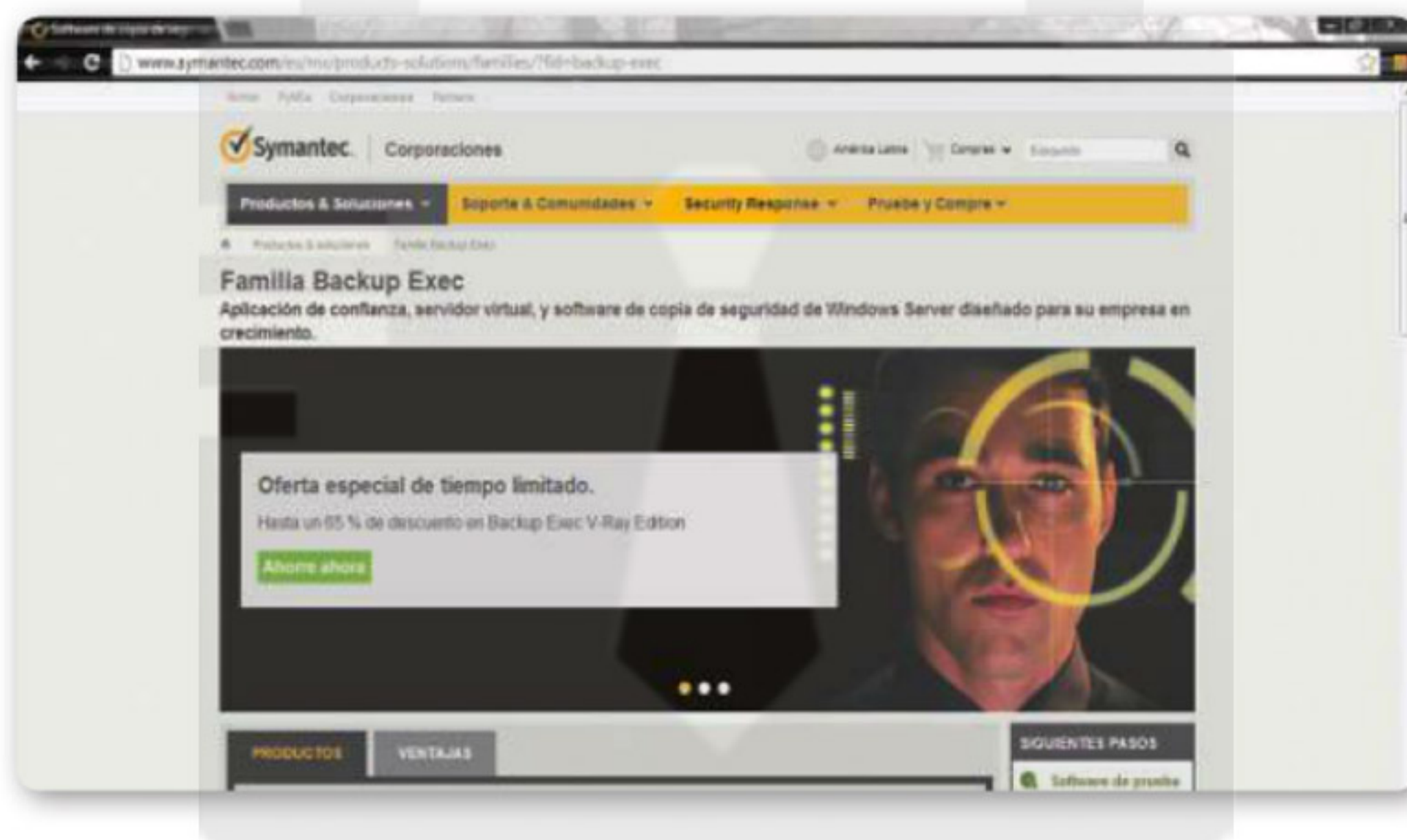


Figura 2. BackupExec es un conjunto de productos para la generación de copias de respaldo, su gestión y la recuperación de datos.

Además, nos permite recuperar sistemas enteros, ya sea Windows o Linux, sobre hardware tanto real como virtual (www.symantec.com).

Como siempre, el uso de herramientas automatizadas nos permitirá ahorrar horas de trabajo y evitar errores, por lo que es fundamental elegir una buena herramienta. Además, debemos tener en cuenta no solo los tipos de datos que queremos resguardar, sino también los que podemos necesitar resguardar en un futuro, porque no todas las herramientas son compatibles con todos los datos o con todos los requerimientos particulares. Por ejemplo, existen algunas particularmente preparadas para realizar copias de seguridad de determinados tipos de

ES UNA BUENA
IDEA ELEGIR
HERRAMIENTAS PARA
SOPORTAR NUEVOS
TIPOS DE DATOS



software, como bases de datos, servidores de correo electrónico, y otros. También es una excelente idea seleccionar una herramienta que pueda ser extendida para soportar nuevos tipos de datos, ya sea que tengamos que hacer el desarrollo nosotros mismos o debemos contratar un consultor especializado. Esto nos permitirá contar con la misma herramienta aunque la infraestructura y los requerimientos cambien.

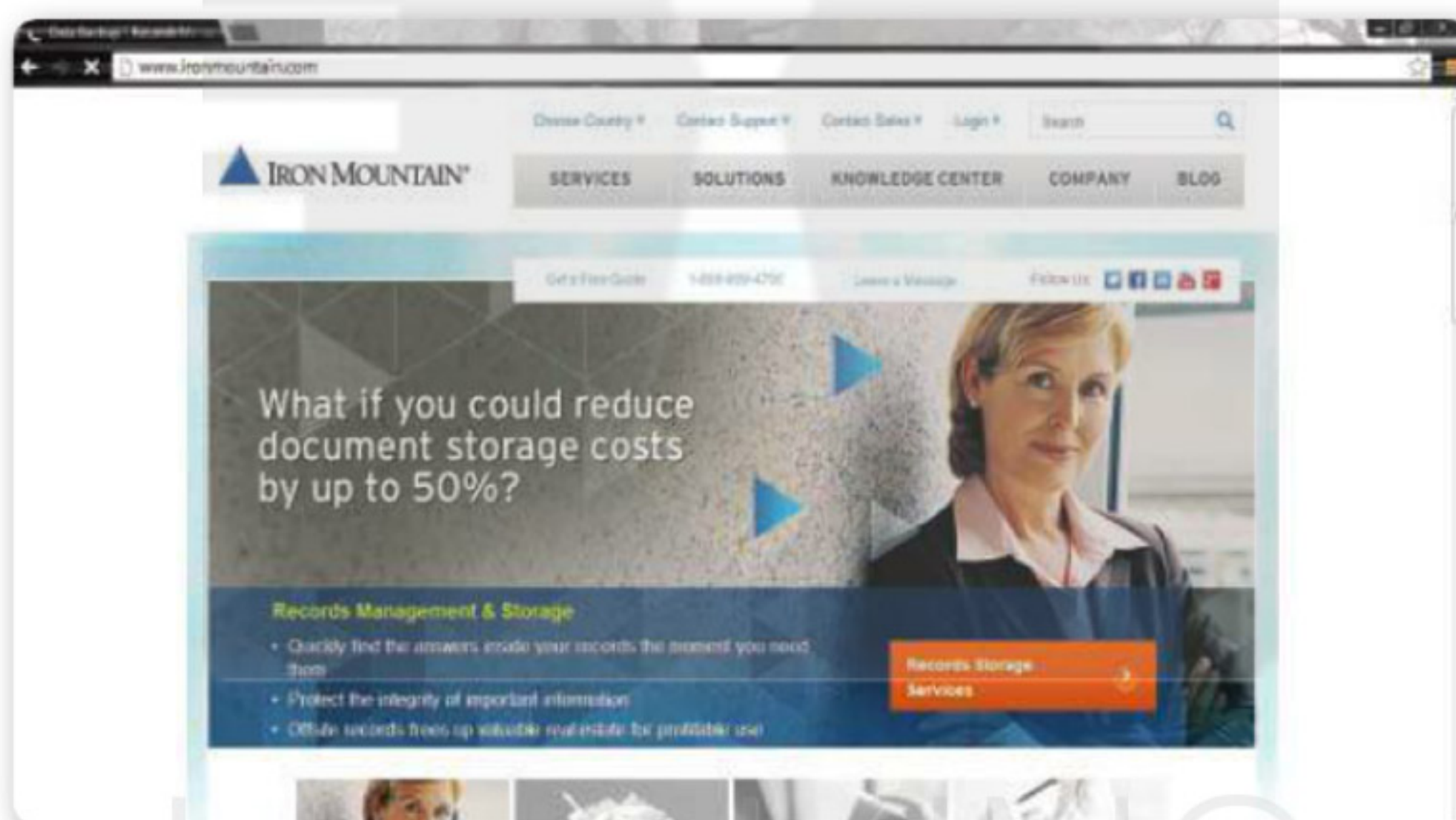


Figura 3. IronMountain es una empresa especializada en la protección de datos y recuperación ante desastres. Publicó un interesante documento llamado “Las cinco mejores prácticas para proteger tus copias de seguridad” (www.ironmountain.com).

Más allá de esto, si no podemos contar con la herramienta perfecta, por lo menos debemos disponer de copias de seguridad realizadas a mano, con la mayor responsabilidad posible. Con el tiempo, y en la medida en que podamos mejorar nuestros procesos, iremos adquiriendo las herramientas adecuadas para efectuar cada tarea, y así optimizar los tiempos y minimizar los errores.

Monitoreo

Un aspecto que nos será de gran utilidad en nuestro trabajo cotidiano, y que nos servirá para impresionar a nuestros jefes, es la posibilidad de conocer rápidamente el estado completo de la infraestructura tecnológica. Esto nos permitirá mantener los problemas a raya, al poder controlar las cosas antes de que sucedan, y asombrará a nuestros superiores, porque demostrará que tenemos el control de la situación, lo cual siempre es bueno.



Figura 4. Zabbix es una excelente herramienta de monitoreo. Escrita en PHP, puede utilizar MySQL y PostgreSQL (www.zabbix.com).



SITIOS RECOMENDADOS

Existen varias herramientas de código abierto destinadas al monitoreo de infraestructuras. Algunas cuentan con versiones comerciales que ofrecen una mayor cantidad de características y tienen soporte del fabricante. Por ejemplo: PandoraFMS (<http://pandorafms.org>), Zabbix (www.zabbix.com), Hyperic (www.hyperic.com) y Zenoss (www.zenoss.com).

Existen varias formas de monitorear una infraestructura, pero la más recomendable es utilizar una herramienta especializada. Esto nos dará la gran ventaja de poder centralizar todo el monitoreo en un solo lugar, ya sea de plataformas Windows, Linux, aplicaciones, y cualquier otro parámetro que queramos seguir de cerca. Como siempre, la selección de la herramienta queda en manos de cada profesional, según sus gustos y necesidades particulares. De esto, lo más importante es hacer la elección sobre la base de toda la estructura, teniendo en cuenta que, en algún momento u otro, necesitaremos monitorear cada uno de nuestros activos de información. Así que al seleccionar dicha herramienta, será preciso tener en cuenta nuestras necesidades tanto actuales como futuras.

Otra de las grandes ventajas que tiene el uso de una herramienta frente a alguna solución más simple, como los típicos scripts de monitoreo, es que en ella podremos definir varios usuarios, y perfiles para cada uno. Con esto, será posible asignar permisos de acceso a cada integrante de la organización, de acuerdo con lo que cada uno necesite. Esta es una ventaja que podemos perder de vista al principio, pero que, luego, se vuelve necesaria si precisamos dividir las tareas de gestión de la seguridad.



Figura 5. Nagios es una de las herramientas de código abierto más populares para el monitoreo de redes y servidores.

Aunque algunas de las características de **Nagios** no son muy actuales, sigue siendo una opción muy potente. La versión paga se encuentra más actualizada y preparada para ofrecer características muy interesantes, además de tener soporte del fabricante (**www.nagios.org**).

Si bien el monitoreo está relacionado directamente con las herramientas de monitoreo de red y servidores, y existen muchas tecnologías y protocolos para realizar estas tareas (como SNMP y WMI), el de seguridad abarca mucho más que eso. Este tipo de herramientas suele basar su funcionamiento en la disponibilidad de los servicios, mientras que como vimos en el **Capítulo 2**, la seguridad también debe considerar la confidencialidad y la integridad. Por lo tanto, necesitamos implementar herramientas complementarias para obtener los datos que buscamos.



Figura 6. La **plataforma PandoraFMS** es una excelente opción para monitorear servidores, equipos de telecomunicaciones y prácticamente cualquier otro dispositivo o servicio de red. Está desarrollada por la empresa española **Artica** (**www.pandorafms.org**).

Algunos de los parámetros que podemos necesitar seguir de cerca, y que se relacionan directamente con la confidencialidad y la integridad de los datos, son los siguientes:

- Modificación de archivos críticos.
- Estado de encriptación de las telecomunicaciones.
- Cantidad de ataques de malware.

Rápidamente podemos darnos cuenta de que estos valores tienen varias diferencias con los parámetros clásicos que se monitorean en una red. Y también observaremos que la obtención de estos valores se realizará por medio de varias fuentes de información, como el software antivirus, los routers y los agentes que tengamos instalados en los servidores. Esto hace que tengamos que integrar varias herramientas, ya sea de forma manual o automatizada, lo que determina que el monitoreo completo de la seguridad informática sea una tarea compleja, que requiere de un planeamiento muy inteligente.

Será cuestión de práctica y experiencia el hecho de ir perfeccionando nuestras capacidades de monitoreo y lograr la integración entre cada una de las herramientas que utilicemos. Con el correr del tiempo, sabremos puntualmente qué valores debemos seguir de cerca y cuáles no son tan importantes.

Control de cambios

Si hay una particularidad que destaca a la tecnología es que cambia constantemente, y esto nos lleva a tener que hacer grandes esfuerzos para



SOLUCIÓN DE MONITOREO



Aunque por diversos motivos no podamos implementar la solución de monitoreo que creamos ideal, es recomendable tener, por lo menos, algo que nos permita estar al tanto de la situación de nuestra infraestructura. No es necesario que sea un sistema avanzado; basta con que se nos envíe un correo electrónico si se detecta una situación anormal.

mantenernos actualizados con lo último del mercado. Justamente, una de las causas más comunes de las nuevas brechas de seguridad y de los desastres en los sistemas informáticos es la pérdida de control sobre los cambios que estos sufren. En la lucha por permanecer actualizados, a veces olvidamos mantener los recaudos de seguridad necesarios.



Figura 7. DeviceExpert es una plataforma para la gestión de configuraciones de dispositivos de red, desarrollada por **Manage Engine** (www.manageengine.com).

Muchas veces se utiliza el concepto de siempre actualizar, como si cada uno de los sistemas debiera estar en su última versión para funcionar



ANALIZAR ANTES DE ACTUALIZAR

Al decidir si hacemos una actualización, debemos tomar en cuenta varios factores, como las nuevas funcionalidades, las mejoras en la seguridad, la estabilidad y la compatibilidad con otros componentes del sistema. No siempre decidiremos hacer las actualizaciones, pero lo más importante es que efectuemos un análisis antes de tomar la decisión.

correctamente o cumplir con las políticas de seguridad. Esta es una verdad a medias, por dos motivos fundamentales. Primero, hay que evaluar si la última versión es considerada estable, porque ciertos equipos de desarrollo suelen publicar versiones de software que son de prueba y que, si bien pueden tener pocos errores, aún no han sido testeadas como para instalarse en equipos de producción. Segundo, las actualizaciones no siempre traen mejoras de seguridad, y muchas veces, presentan más requerimientos de hardware o dependencias de software. Por eso, es preciso tener cuidado al decidir si aplicamos las actualizaciones o no.



Figura 8. Puppet es una herramienta para la gestión de configuraciones de sistemas de tipo UNIX. Está desarrollada en **Ruby**, cuenta con una gran comunidad de usuarios y dispone de varios recursos de documentación (www.puppetlabs.com).

Por otro lado, también tenemos los cambios de configuraciones, que suelen hacerse en equipos de producción, sin tener en cuenta que pueden provocar caídas del sistema, problemas de rendimiento y hasta pérdidas de datos. Para este tipo de situaciones, también podemos contar con herramientas que nos permitan mantener distintas versiones de las configuraciones del sistema. Lamentablemente, como cada sistema utiliza su

propio método de configuración (bases de datos, archivos de texto plano, archivos XML, formatos propietarios, ldap, etc.), es muy difícil encontrar una única herramienta con la cual mantener todas nuestras configuraciones. En este caso, todo dependerá de nuestras necesidades, de nuestra creatividad y de nuestra capacidad para desarrollar herramientas propias, mezclándolas con las ya existentes. También debemos analizar los criterios para seleccionar los productos que vamos a implementar, teniendo en cuenta los métodos de configuración disponibles, a fin de simplificar el mantenimiento y la gestión de las configuraciones.

Ambientes de pruebas y producción

Cuando nos encontramos frente a la situación de tener que implementar una modificación –ya sea por una actualización de software o hardware, o por un cambio de configuración–, sabemos que existe el riesgo de provocar una caída en el sistema o la pérdida de datos. Es por eso que se vuelve extremadamente recomendable contar con un ambiente de pruebas idéntico al de producción, que nos sirva para probar los cambios y verificar que todo funcione correctamente.

De ser posible, debemos tener un sistema de pruebas por cada sistema de producción. Si no disponemos de los recursos necesarios, como mínimo necesitaremos sistemas de pruebas que se correspondan con los sistemas de producción más críticos. Para esto, podemos hacer uso de la virtualización, que nos permitirá crear equipos virtuales de pruebas en pocos minutos.

Es importante entender que un equipo de pruebas no deja de ser un equipo de nuestra infraestructura, y debe ser protegido como tal. Para esto, tendremos que implementar las políticas de seguridad correspondientes y tratar de mantenerlo lo más aislado posible de los equipos de producción, de modo que no haya ningún tipo de inconveniente entre ellos. Además, es necesario que cada equipo de pruebas tenga bien identificado su rol de pruebas, y no sea utilizado para absolutamente ninguna tarea de producción.



Gestión de incidentes

Cuando ocurre un incidente de seguridad, lo más importante es saber exactamente qué hacer. De acuerdo con la gravedad del asunto, tal vez tengamos que reaccionar de manera inmediata, con lo cual será de suma importancia tener a mano las herramientas y la información correctas.

Es ampliamente recomendable contar con un sistema de seguimientos de incidentes, a fin de registrar cada uno de los problemas que van surgiendo, con sus respectivas soluciones. Esto nos dará la posibilidad de hacer un análisis estadístico de nuestros tiempos de respuesta y de los problemas más frecuentes.

Para definir la criticidad de un incidente, debemos basarnos en la clasificación de activos, analizando a cuáles afecta y qué problemas produce. Esto también nos permitirá saber de qué tenemos que ocuparnos primero si se presentan varios incidentes al mismo tiempo o hay varios activos afectados.



Figura 9. Mantis es una herramienta que nos permite mantener un registro de incidentes, hacer seguimientos y reportes, y muchas otras tareas más. Es bastante personalizable y, por si esto fuera poco, es de código abierto, está escrita en PHP y utiliza una base de datos MySQL (www.mantisbt.org).

También existen herramientas que integran el monitoreo con la prevención de intrusos, el seguimiento de incidentes y otras funciones de seguridad. Se las denomina SIEM (*Security Information and Event Management*).



Figura 10. Prelude es un **SIEM** de código abierto bastante interesante, que puede obtener datos de diversas fuentes, como Snort, OSSEC y otras herramientas de detección de intrusos, así como de herramientas de monitoreo (www.prelude-technologies.com).

Las herramientas del tipo SIEM suelen ser complejas, y puede llevar un tiempo configurarlas correctamente y acostumbrarnos a utilizarlas. Pero, una vez que dominemos su uso, pueden ahorrarnos muchísimo tiempo y brindarnos la capacidad de centralizar una gran cantidad de tareas en un mismo lugar. Además, suelen estar preparadas para conectarse con herramientas externas, lo que las convierte en un excelente recurso para la gestión de grandes infraestructuras, que cuentan con sistemas que obligan a los administradores a utilizar herramientas diferentes.

LAS HERRAMIENTAS
SIEM PUEDEN
REQUERIR MUCHO
TIEMPO DE
CONFIGURACIÓN



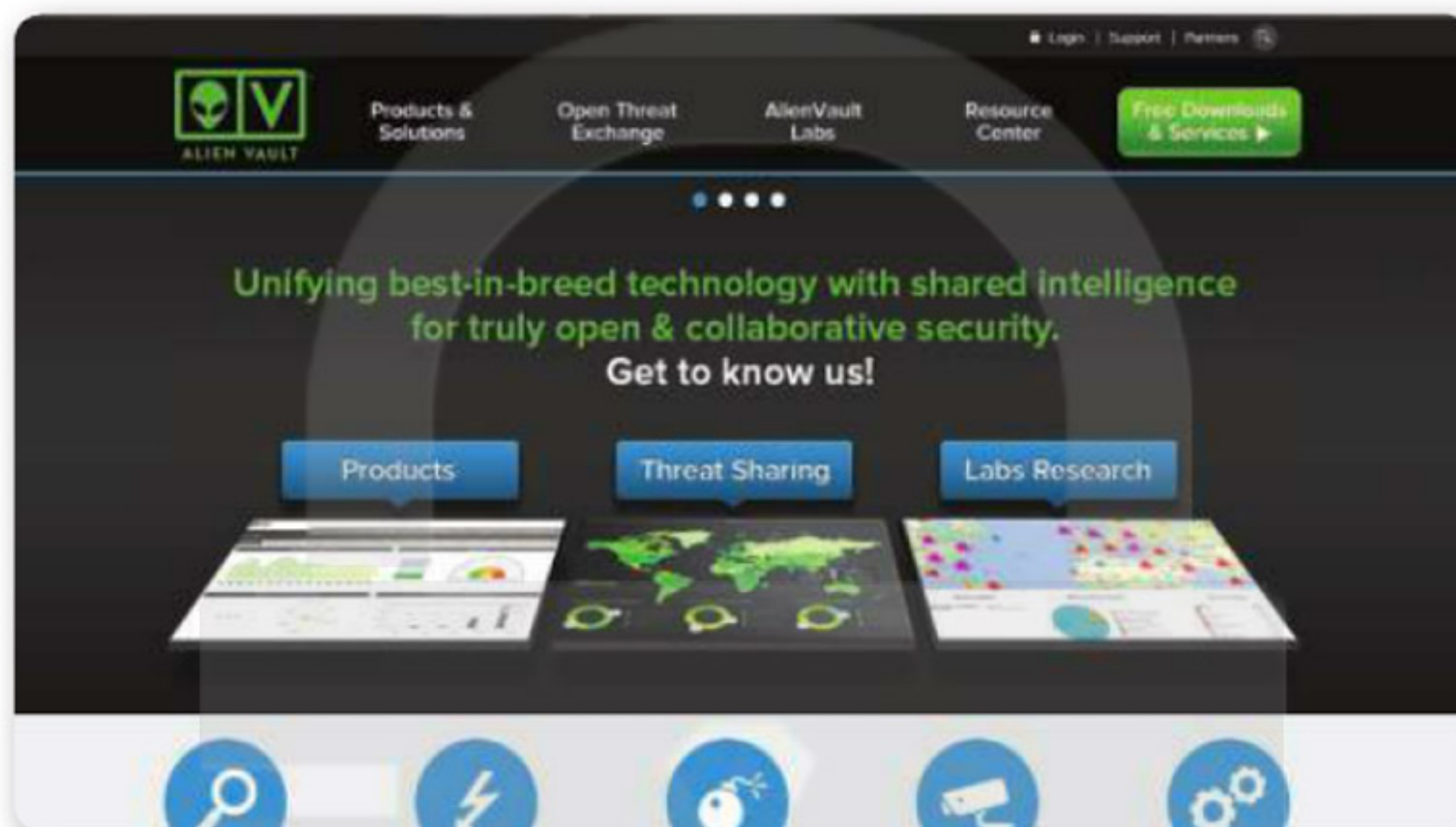


Figura 11. OSSIM es un SIEM desarrollado por la empresa AlienVault, que se basa en la agrupación de varias herramientas de código abierto, como Snort, Nagios, OpenVas y algunas otras. Cuenta con una versión paga que ofrece algunas capacidades extra, además del soporte del fabricante (<http://alienvault.com>).

Es una excelente idea probar este tipo de sistemas, utilizarlos durante un tiempo y ver con cuál nos sentimos cómodos, analizando qué beneficios podemos tener a corto y largo plazo.

Los SIEM pagos suelen tener precios elevados, así que tendremos que pensarlo bien antes de tomar una decisión. Todo dependerá de la cantidad de recursos con los que contemos para llevar a cabo la gestión de la seguridad. Si disponemos de buenos recursos económicos pero estamos acotados en cuanto a recursos humanos, la instalación de un SIEM puede optimizar todas nuestras tareas, lo cual puede terminar siendo un ahorro de dinero para la organización. Además, este tipo de herramientas suele dar la posibilidad de generar reportes, los cuales nos servirán para los procesos de análisis y mejora continua.

Debemos tener en cuenta que, más allá de las herramientas que podamos utilizar, la gestión de incidentes no deja de ser otra cosa que estar al tanto de todo lo que sucede en nuestra infraestructura y enterarnos, de una forma u otra, de todo lo que ocurra con la mayor rapidez posible. Una

vez detectados, los incidentes deben resolverse en tiempo y forma. En resumen, la gestión de incidentes es el conjunto de políticas, metodologías, herramientas y procedimientos que deben llevarse a cabo para lidiar con todos los eventos adversos que pueden suceder en nuestros sistemas.

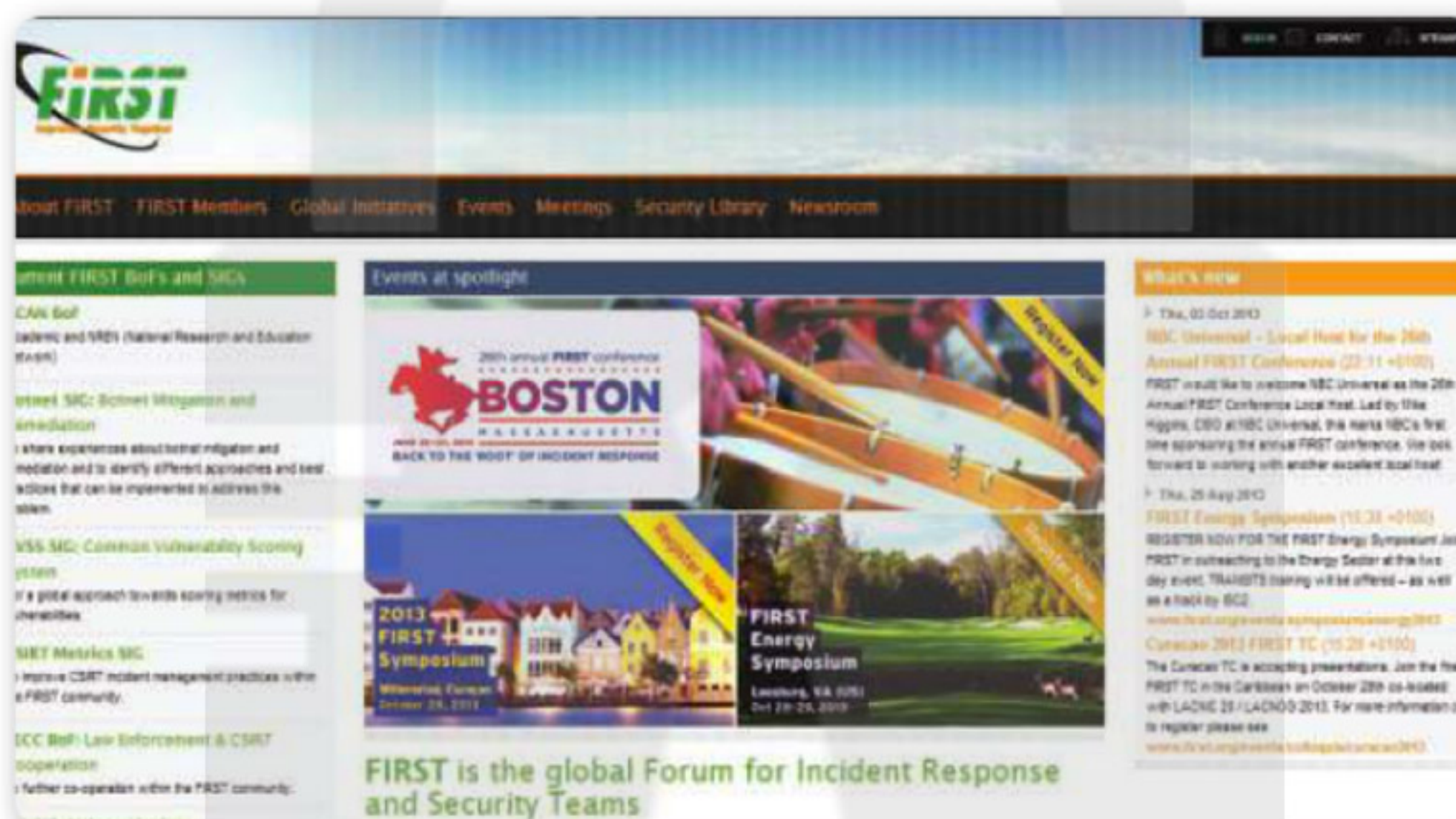


Figura 12. El Foro de Equipos de Respuesta a Incidentes de Seguridad (**FIRST**) es una entidad que organiza a varios de los equipos de respuesta a incidentes (**CERT**) del mundo.

Allí podemos encontrar diversos recursos de interés (www.first.org).



BIA, BCP y DRP

Cuando nos ponemos a pensar en todo lo malo que puede ocurrirles a nuestros sistemas, solamente hay una cosa que puede mantenernos tranquilos: tener un plan. Y, si bien es cierto que no podemos estar preparados para responder ante absolutamente todas las cosas que pueden suceder, el hecho de saber que estamos preparados para afrontar las situaciones adversas más probables no solo nos da seguridad, sino que también nos obliga a conocernos mejor.

Un punto clave al responder ante una emergencia es la frialdad con la que lo hacemos, porque la presión sobre nosotros puede hacernos actuar de manera equivocada. Es por eso que muchas veces, al tratar de reparar un desastre, producimos otro mucho mayor. Por lo tanto, en las situaciones de estrés que no nos permiten pensar es necesario tener un plan que lo haga por nosotros.

La **organización DRI International** se encarga de promover las actividades de continuidad de negocio y recuperación de desastres a través de educación, asistencia y publicación de documentación relevante.



Figura 13. Aunque la **organización DRI International** no se enfoca directamente en la seguridad informática, es un excelente recurso de información (www.drii.org).

Las siglas BIA, BCP y DRP hacen referencia a *Business Impact Analysis*, *Business Continuity Plan* y *Disaster Recovery Plan*, respectivamente.

El BIA (o análisis de impacto en el negocio) es el estudio que indica cuáles serían las situaciones que tendrían un impacto más negativo en la operatoria de una organización. Suele ser un estudio que no considera solamente la tecnología, sino que abarca todas las posibilidades, como desastres naturales, problemas de imagen, muerte de personal de puestos críticos, cambios en la economía local y global, etcétera.

El proceso de desarrollo de este tipo de documentos es complejo, y abarca cuestiones que van mucho más allá de la seguridad informática, así que no vamos a detenernos mucho en este tema. Pero a continuación mostramos un listado de los pasos clave para poder crear un documento de estas características:

1. Seleccionar a los individuos que vamos a consultar.
2. Elegir las técnicas para obtener datos (cuestionarios, entrevistas, etcétera).
3. Identificar las funciones críticas del negocio.
4. Identificar los recursos que son necesarios por estas funciones.
5. Calcular durante cuánto tiempo pueden sobrevivir estas funciones sin esos recursos.
6. Identificar las vulnerabilidades y amenazas para estos recursos.
7. Calcular el riesgo asociado a cada función del negocio.
8. Documentar los datos encontrados y reportarlos a la gerencia.

Como podemos observar, el proceso de desarrollo del BIA es muy similar a lo que vimos en el análisis de riesgos. La particularidad que tiene es que debemos considerar cualquier tipo de amenaza, no solo las relacionadas directamente con la información y la tecnología.



EVENTOS ADVERSOS INIMAGINABLES



Tomando como ejemplo un evento catastrófico, los ataques terroristas del 11 de septiembre de 2001 al World Trade Center, no solo implicaron la pérdida de vidas, sino que también destruyeron negocios por completo y dejaron a muchas empresas al borde de la quiebra. Muchas de ellas contaban con todos sus recursos apostados en un mismo lugar, tanto los humanos como los tecnológicos, y por eso no pudieron resistir la catástrofe. Esto nos demuestra que la cantidad de eventos adversos que podrían llegar a ocurrirnos es infinita.

Para simplificar nuestro trabajo, analizaremos el caso de una unificación de estos dos documentos, que resulta en un único BCP/DRP. Para las organizaciones que lo requieran (son verdaderamente pocas), será necesario hacer un estudio minucioso y elaborar todo un proyecto para definir tanto un BIA, como un BCP y un DRP.



Figura 14. En el sitio del **Business Continuity Institute** podemos encontrar recursos acerca de las mejores prácticas para la continuidad del negocio, además de referencias a cómo obtener la certificación BCI (www.thebci.org).

Pensando en una organización pequeña o mediana (y hasta en una organización grande, pero que tenga una estructura simple), nosotros vamos a trabajar sobre los datos obtenidos en el **Capítulo 2** (para evitar el desarrollo de un BIA) y a unificar la continuidad de nuestro negocio a través de un único documento BCP/DRP. Podemos decir que los puntos clave para el desarrollo del documento BCP/DRP son los siguientes:

1. Definir el proyecto para desarrollar el BCP/DRP. Asignar los roles, responsabilidades y autoridades de cada uno de los involucrados en el proceso. De este paso depende gran parte del orden con el cual se desarrollará el proyecto.

2. Sobre la base del análisis de riesgos, identificar las amenazas y vulnerabilidades que podrían llegar a desencadenar un desastre. Esto nos va a servir para encaminar el proyecto y asignar prioridades a nuestras acciones.
3. Desarrollar estrategias de recuperación para cada una de las situaciones identificadas, tratando de unificar las medidas de recuperación, para reducir costos y simplificar el plan.
4. Escribir el plan de contingencia, con sus respectivos procedimientos y la asignación de roles para cada uno de los integrantes que deben intervenir en el proceso. Además, hay que explicar detalladamente cómo seguirá funcionando la organización mientras se recupera del desastre.
5. Probar el plan, realizar ejercicios de entrenamiento y capacitaciones. Esto es de vital importancia para asegurar que el plan funciona correctamente, y tener a los empleados bien preparados para responder en tiempo y forma.
6. Mantener el plan, tanto con actualizaciones periódicas, como buscando las formas de optimizar el documento, los procedimientos y a las personas involucradas. Si no hacemos esto, al cabo de poco tiempo, el plan quedará desactualizado y no nos servirá de nada.

ES NECESARIO
IDENTIFICAR
LAS AMENAZAS
Y RIESGOS
POTENCIALES



DOCUMENTOS BCP Y DRP



Como los documentos BCP y DRP cumplen funciones bastante similares, podemos darnos el lujo de unificar el contenido de ambos en uno solo, siempre y cuando nuestra organización lo amerite. Por lo general, pueden unificarse en pequeñas y medianas empresas, y deben estar separados en grandes organizaciones, que tienen una estructura más compleja.

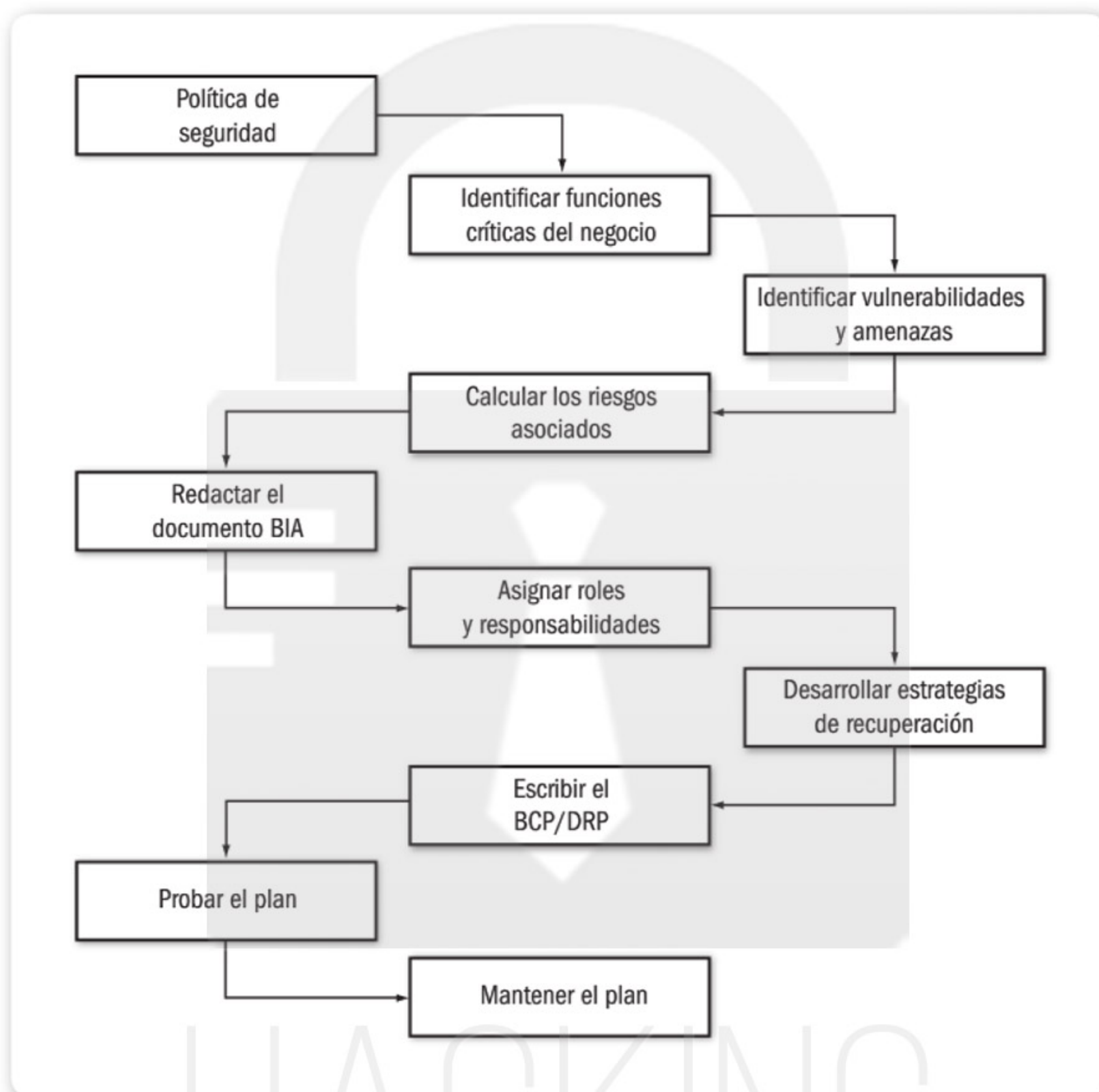


Figura 15. El gráfico muestra los principales pasos que deben llevarse a cabo en el desarrollo y mantenimiento de un BCP/DRP. Es un proceso complejo, porque cada uno de los puntos mencionados lleva tiempo y tiene varias tareas asociadas.

Sitios de contingencia

Ya sea porque una normativa nos lo pide o porque hemos evaluado que es imprescindible, puede ser necesario contar con un sitio de contingencia, que sirva para alojar sistemas de respaldo en caso de que los sistemas

principales sufran daños. Este tipo de medidas es muy recomendable si queremos asegurar que podremos continuar con la operatoria de la organización en situaciones catastróficas.

La decisión de invertir en un sitio de contingencia debe salir del análisis de riesgos o del análisis de impacto en el negocio (BIA). Una vez que reconocemos la necesidad de un sitio de contingencia, nos queda seleccionar el tipo de sitio y el lugar en el que se encontrará. Los siguientes son los tres tipos de sitios entre los que deberemos elegir:

Sitio de contingencia en frío (cold site)

Este tipo de sitios contiene la estructura básica, con electricidad, cableado y aire acondicionado, pero solamente eso; no incluye ningún equipamiento informático. Es la opción más económica, pero toma más tiempo en volverse operativa, porque tendremos que conseguir el equipamiento en el momento del desastre y configurarlo adecuadamente.

Sitio de contingencia tibio (warm site)

Este tipo de sitios, además de contener lo mismo que uno frío, cuenta con algunos dispositivos informáticos, generalmente genéricos, como servidores, estaciones de trabajo y equipamiento de redes. Tarda menos tiempo en volverse operativo que un sitio frío, pero aun así, deberemos configurar los equipos y tal vez tengamos que conseguir el hardware que nos es provisto por él. En algunas organizaciones que utilizan mainframes, servidores especiales o equipos de telecomunicaciones avanzados, podríamos tener que llevarlos y configurarlos.

Sitio de contingencia caliente (hot site)

Este tipo de sitios está completamente equipado y puede ponerse en marcha en pocas horas. Lo único que suele faltar en estos casos son los datos. El equipamiento instalado en ellos debe ser completamente compa-

tible con el del sitio original. Obviamente, es la opción más costosa, sobre todo si necesitamos que haya hardware muy particular o muy potente, pero nos garantiza la transición menos agresiva de un sitio a otro.

	Ventajas	Desventajas
Cold Site	• Es el más económico.	• Tarda mucho tiempo en volverse productivo. • Tenemos que llevar todo el equipamiento informático.
Warm Site	• Relación costo/beneficio. • Pueden probarse con relativa facilidad.	• Tenemos que llevar ciertos equipos informáticos.
Hot Site	• Disponible inmediatamente. • Las pruebas son fáciles de realizar.	• Costo muy elevado.

Figura 16. La tabla muestra, a grandes rasgos, las ventajas y desventajas de cada uno de los tipos de sitio de contingencia. Nuestra elección dependerá tanto del análisis de estos factores, como de nuestras necesidades y recursos disponibles.

Para la selección del tipo de sitio adecuado tendremos que analizar qué tiempos de caída de servicio podemos tolerar, las probabilidades de que



PLAN DE CONTINGENCIAS



Debemos tener en cuenta que pese a todas las medidas de seguridad que implementemos, puede ocurrir un desastre. Por esta razón hay que definir un plan de recuperación de desastres para cuando falle el sistema. Es necesario que nuestro plan de contingencias incluya un completo plan de recuperación ante cualquier desastre.

ocurra un desastre y los recursos económicos de los que disponemos.

La opción más utilizada son los sitios tibios, que suelen permitir un buen balance entre tiempos de respuesta y costo.

En el caso de las organizaciones que no puedan soportar ni siquiera un día de pérdida de servicio, será necesaria la contratación de un sitio caliente.

De todos modos, cualquiera de las opciones elegidas debe ser verificada periódicamente, para corroborar que los procesos de recuperación y el equipamiento del sitio funcionan como corresponde. Además, estas pruebas nos darán una buena idea de cuáles son nuestros tiempos de recuperación.

En caso de contar con varios centros de procesamiento de datos, es una excelente idea que uno sea respaldo de otro, lo que nos permitirá ahorrar costos, porque, de todas formas, la organización tiene que mantener esos sitios. De todos modos, si elegimos esta opción, tendremos que asegurarnos de que los recursos –tanto de hardware como de espacio– permitan que un centro de procesamiento de datos se vuelva rápidamente en sitio de respaldo, y deberemos hacer pruebas periódicas referidas al funcionamiento del plan. Esta opción suele ser la más económica, pero es aplicable solo a las organizaciones que cuentan con más de un centro de procesamiento.



RESUMEN



En este capítulo hemos analizado la forma en que debemos realizar copias de respaldo de los archivos importantes de nuestra organización, y también conocimos los aspectos importantes del monitoreo de los problemas de seguridad que puedan presentarse. Para continuar, vimos las particularidades del control de cambios y revisamos algunas herramientas de software que pueden apoyarnos en esta tarea. Finalmente, conocimos los conceptos de BIA, BCP y DRP y mencionamos los sitios de contingencia.

Actividades

TEST DE AUTOEVALUACIÓN

- 1 ¿Sobre la base de qué criterios debemos seleccionar los datos por respaldar y la frecuencia entre respaldos?
- 2 ¿Qué diferencia existe entre el monitoreo convencional de infraestructuras tecnológicas y el monitoreo de seguridad?
- 3 ¿Por qué se vuelve difícil unificar la gestión de las configuraciones de los distintos componentes de una infraestructura?
- 4 ¿Por qué es importante saber de antemano cómo reaccionar ante un evento adverso?
- 5 ¿Cuáles son las características de los distintos tipos de sitios de contingencia?



PROFESOR EN LÍNEA



Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: **profesor@redusers.com**

Telecomunicaciones

En este capítulo veremos la importancia de los distintos tipos de dispositivos de telecomunicaciones, evaluaremos las ventajas y desventajas de implementar firewalls y sistemas IDS, y también aprenderemos a seleccionar la mejor forma de administrar nuestros dispositivos.

▼ Introducción.....	92	▼ Implementación de sistemas IDS.....	114
▼ Inventario de dispositivos	93	▼ Administración remota	114
▼ Routers y switches	96	▼ Protocolos TCP/IP	119
▼ Firewalls	103	▼ Diseño de redes seguras.....	130
▼ Redes inalámbricas	106	▼ Resumen.....	137
▼ Prevención de intrusos	110	▼ Actividades.....	138





Introducción

Las **redes de computadoras** ya no son cosa del futuro, sino que están establecidas como algo común y corriente, casi implícitas en toda organización. Son un recurso tan habitual como el papel, y las empresas las utilizan para transportar datos a velocidades que, hasta hace unos años, eran imposibles de imaginar. Todas estas tecnologías simplifican la vida de cada uno de los integrantes de una organización.

Al plantear las estrategias de seguridad, la mayoría de las empresas tienden a enfocarse en las estaciones de trabajo y los servidores, porque estos son los equipos que almacenan y procesan la información con la que se trabaja día a día. Así que es común olvidar los dispositivos, las tecnologías y los protocolos que llevan esa información de un lugar a otro. Esto hace que, muchas veces, existan graves vulnerabilidades de seguridad, que no son detectadas hasta que algo malo sucede. Es por eso que cobra tanta importancia la visión global de la seguridad informática, que nos permite proteger una organización como un todo, y nos da la posibilidad de utilizar cada uno de nuestros dispositivos como una herramienta más de seguridad, en vez de verlos como puntos de falla. Recordemos que todo pasa por estos equipos, de modo que no podemos darnos el lujo de perder la oportunidad de controlarlos por completo, para sacar el máximo provecho de ellos.

Como expertos en seguridad, debemos tener una comprensión clara de las tareas que cumple cada uno de los dispositivos, así como también de los beneficios y las vulnerabilidades que pueden introducir en nuestra infraestructura. Es imposible evitar el uso de estos equipos, así que tendremos que aprender a seleccionarlos, configurarlos y mantenerlos de la manera adecuada.

Es por eso que debemos tener en claro, exactamente, cuáles son las herramientas y los recursos que tenemos a mano para prevenir y dar respuesta a los inconvenientes que surjan en esta área de la seguridad. En las siguientes páginas analizaremos en qué forma debemos proteger nuestras redes y qué herramientas podemos utilizar para simplificar nuestras tareas.





Inventario de dispositivos

Como vimos en el **Capítulo 2**, contar con un inventario de los dispositivos que se encuentran en una red es de vital importancia para poder implementar correctamente las medidas de seguridad adecuadas.

Para este tipo de tareas existen varias herramientas, muchas de ellas, de código abierto, como **Wireshark**, **Arpwatch**, **Ettercap**, y otras. Podemos ejecutarlas constantemente, y automatizarlas para obtener un reporte constante de los nuevos dispositivos que aparecen en nuestra red. A continuación, analizaremos algunas formas de llevar a cabo esta tarea.

UN INVENTARIO
DE DISPOSITIVOS
ES VITAL PARA LA
SEGURIDAD
DE LA RED



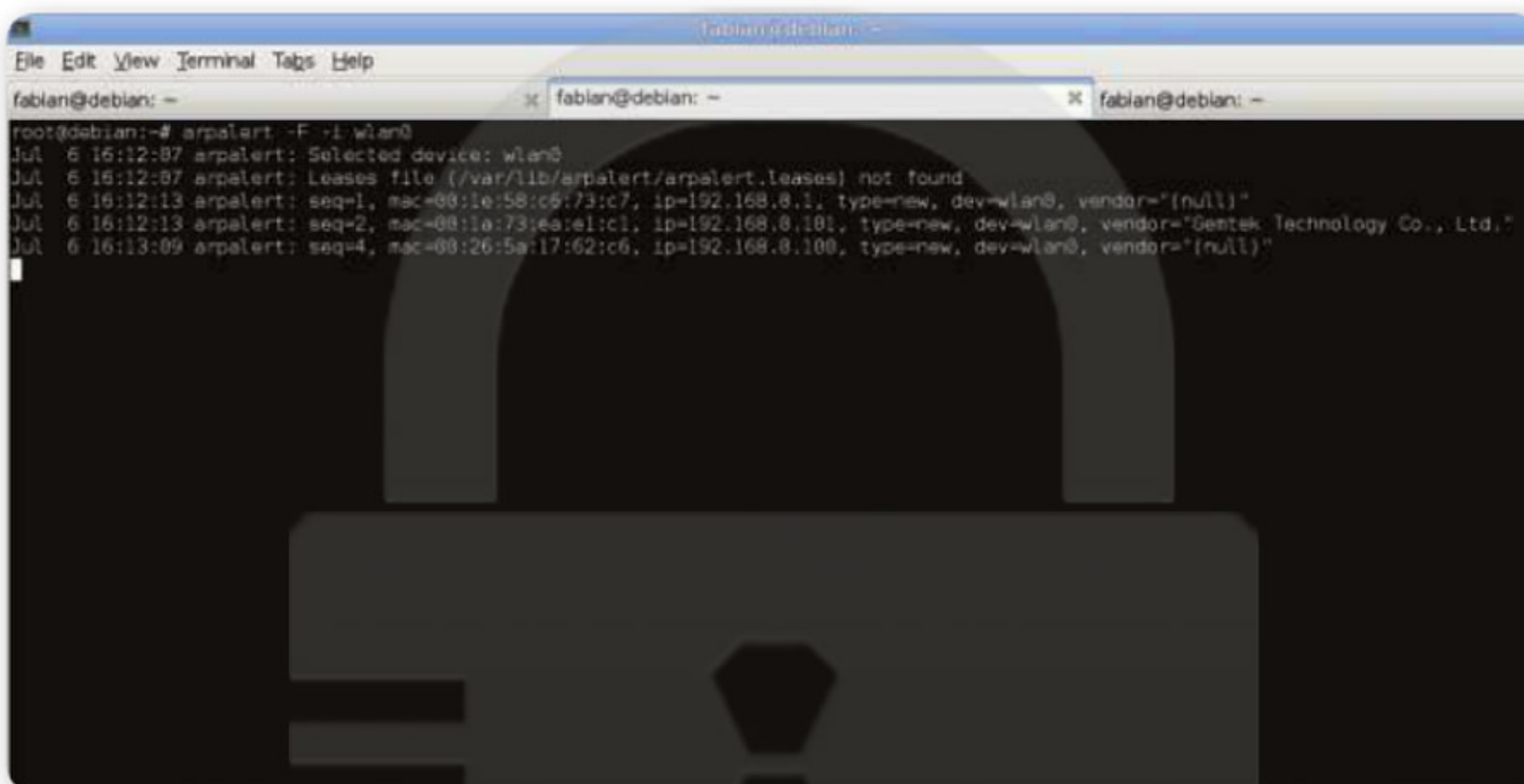
Switches inteligentes

En caso de contar con **switches inteligentes**, podemos utilizar tecnologías como **Port Security** (presente en los dispositivos **Cisco**), que permite enviar una notificación a través de un **Trap SNMP** acerca de las nuevas **MAC** aparecidas en un puerto.

Arpalert

Esta herramienta nos permite capturar el tráfico de una interfaz de red, y detectar las asociaciones de **IP** y **MAC actuales**, notificándonos de nuevos dispositivos y otro tipo de cambios. Es una herramienta de código abierto muy útil, que puede servirnos para crear rápidamente el inventario que corresponde a una red.

Trabaja analizando los paquetes del tipo **ARP**, que se envían normalmente en una red para conocer la dirección MAC asociada a una IP. Como estos paquetes se mandan a todos los hosts de la red, podemos verlos y detectar de forma sencilla cuáles son los dispositivos activos.



```
fabian@debian: ~  
root@debian:~# arpalert -F -i wlan0  
Jul 6 16:12:07 arpalert: Selected device: wlan0  
Jul 6 16:12:07 arpalert: Leases file (/var/lib/arpalert/arpalert.leases) not found  
Jul 6 16:12:13 arpalert: seq=1, mac=08:1e:58:c6:73:c7, ip=192.168.0.1, type=new, dev=wlan0, vendor='{null}'  
Jul 6 16:12:13 arpalert: seq=2, mac=08:1a:73:ea:el:c1, ip=192.168.0.101, type=new, dev=wlan0, vendor='Gentek Technology Co., Ltd.'  
Jul 6 16:13:09 arpalert: seq=4, mac=08:26:5a:17:62:c6, ip=192.168.0.100, type=new, dev=wlan0, vendor='{null}'
```

Figura 1. Arpalert es un software que nos alerta de cambios entre las asignaciones MAC/IP, lo cual puede ser muy útil como complemento a otras herramientas de monitoreo (www.arpalert.org/arpalert.html).

Scripting

Por último, podemos implementar una solución personalizada, au-

PODEMOS
IMPLEMENTAR
SOLUCIONES
AUTOMATIZADAS
COMO ARPALERT

tomatizando herramientas como Arpalert o creando otras propias, a través de librerías como **Scapy**, que fue creada para el lenguaje de programación Python.

Este tipo de pequeños programas puede ser de gran utilidad, porque nos permiten realizar tareas sencillas, y formular reportes, enviar correos electrónicos con notificaciones, y cualquier otra cosa que podamos necesitar.



Es necesario tener ciertos conocimientos sobre programación para desarrollarlos nosotros mismos, aunque podemos encontrar en internet varios ejemplos y scripts completos, listos para utilizar.



Scapy

- [Security Power Tools](#) was out in August 2007. I wrote a complete chapter on [Scapy](#).
-  Scapy trainings at CanSecWest, EuSecWest, PacSec: [NEXT SESSION: CanSecWest march 7th and 8th, 2011](#)
- I can give trainings on many subjects ([Scapy](#), networks, shellcoding, exploit writing, etc.). Contact me directly: phil@secdev.org
- If you like what I do, you can [Donate](#)

About Scapy

What is Scapy

Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and more. It can easily handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery (it can replace hping, 85% of nmap, arpspoof, arp-sk, arping, tcpdump, tethere, etc.). It also performs very well at a lot of other specific tasks that most other tools can't handle, like sending invalid frames, injecting your own 802.11 frames, combining techniques (VLAN hopping+ARP poisoning, VoIP decoding on WEP encrypted channel, ...), etc. See [interactive tutorial](#) and [the quick demo: an interactive session \(some examples may be outdated\)](#).

What makes scapy different from most other networking tools

First, with most other tools, you won't build something the author did not imagine. These tools have been built for a specific goal and can't deviate much from it. For example, an ARP cache poisoning won't let you use double 802.1q encapsulation. Or try to find a program that can send, say, an ICMP packet with padding (I said padding, not payload, see?). In fact, each time you have a new need, you build a new tool.

Second, they usually confuse decoding and interpreting. Machines are good at decoding and can help human beings with that. Interpretation is reserved to human beings. Some programs try to interpret behaviour. For instance they say "this port is open" instead of "I received a SYN-ACK". Sometimes they are right. Sometimes not. It's easier for beginners, but when you know what you're doing, you're trying to deduce what really happened from the program's interpretation to make your own, which is hard because you lost a big amount of information. And you often end up using `tcpdump -x` to decipher what the tool missed.

Third, even programs which only decode do not give you all the information they received. The network's vision they give you is the one their author thought was sufficient. But it is not complete, and you're biased. For instance, do you know a tool that reports the padding?

Scapy tries to overcome those problems. It enables you to build exactly the packets you want. Even if I think stacking a 802.1q layer on top of TCP has no sense, it may have some for somebody else or some product I don't know. Scapy has a flexible model that tries to avoid such arbitrary limits. You're free to put any value you want in any field you want, and stack them like you want. You're an adult and you know what you're doing.

In fact, it's like building a new tool each time, but instead of dealing with a hundred line C program, you only write 2 lines of Scapy.

After a probe (scan, traceroute, etc.) Scapy always gives you the full decoded packets from the probe, before any interpretation. That means that you can probe once and interpret many times, like `tracert` and look at the padding for instance.

Figura 2. Scapy es una librería para el lenguaje de programación Python, que simplifica la tarea de crear paquetes de red personalizados (www.secdev.org/projects/scapy).

Para demostrar la potencia de Scapy, abajo tenemos un script que nos alerta de todas las consultas ARP que se realizan en una red. Con algunas pequeñas modificaciones, podríamos obtener un programa similar a Arpalert, contenido en solo algunas líneas de código.

```
#!/usr/bin/env python
from scapy.all import *

def arpmon(pkt):
    if ARP in pkt and pkt[ARP].op in (1,2):
        return pkt.printf("%ARP.hwsrc% %ARP.psrc%")

sniff(prn=arpmon, filter="arp", store=0)
```


Routers y switches

Si bien existen varios tipos de dispositivos de telecomunicaciones, los routers y los switches son, sin dudas, los más utilizados en la mayoría de las empresas. Tanto en equipos de gama alta como en los de gama baja, debemos considerar aspectos de seguridad al seleccionarlos, instalarlos y configurarlos, para proteger nuestros datos de la manera adecuada.



Figura 3. Cisco Systems es uno de los fabricantes de equipos de telecomunicaciones más reconocidos (www.cisco.com).



SCRIPTS

Aprender a programar scripts es de vital importancia para convertirnos en excelentes profesionales. Seguramente, pasaremos por diversas situaciones en las cuales este tipo de conocimientos puede simplificar en gran medida nuestras tareas. Y no es algo difícil de aprender: es cuestión de elegir un lenguaje y practicar. Para comenzar, es recomendable trabajar con Python.



Los switches son un caso especial, aún más olvidado, en general, porque hasta hace unos años los dispositivos que trabajaban en la capa 2 del modelo OSI no eran gestionables ni configurables. Eso hizo que se los considerara como una especie de adaptador básico, que permitía unir varios dispositivos, así como lo hace el adaptador eléctrico, que nos permite conectar la televisión, la radio y el reproductor de DVD en un mismo enchufe. Debemos considerar que esto ha cambiado, y tenemos que ponernos al corriente; por ejemplo, los switches se presentan como dispositivos cada vez más inteligentes, y por lo tanto, importantes para la implementación de una red de datos.

Como primera medida, y como hemos visto en los capítulos anteriores, debemos mantener un inventario de cada uno de nuestros dispositivos de comunicaciones. Para hacerlo, podemos recurrir a varios protocolos, de los cuales el más estandarizado y presente en todos los dispositivos del mercado es SNMP (*Simple Network Management Protocol*). Algunos fabricantes tienen sus propios protocolos, como es el caso de Cisco con CDP. Sea cual sea el protocolo o la herramienta que utilizemos, es importante tener un inventario y estar al tanto del estado de cada uno de los equipos que componen la red.

Debemos ser cuidadosos con respecto a los puertos y servicios que habilitamos en nuestros dispositivos, y tratar de que sea la menor cantidad posible, además de configurar adecuadamente las interfaces de administración para asegurarlas como corresponde.



CONFIGURACIÓN DE DISPOSITIVOS



No es necesario tener conocimientos avanzados sobre configuración de dispositivos de red, porque este es un tema bastante complejo. Pero es estrictamente imprescindible tener buenos conocimientos acerca de los protocolos más utilizados, como TCP/IP, y de los posibles problemas de seguridad que pueden presentar, así como de sus soluciones.

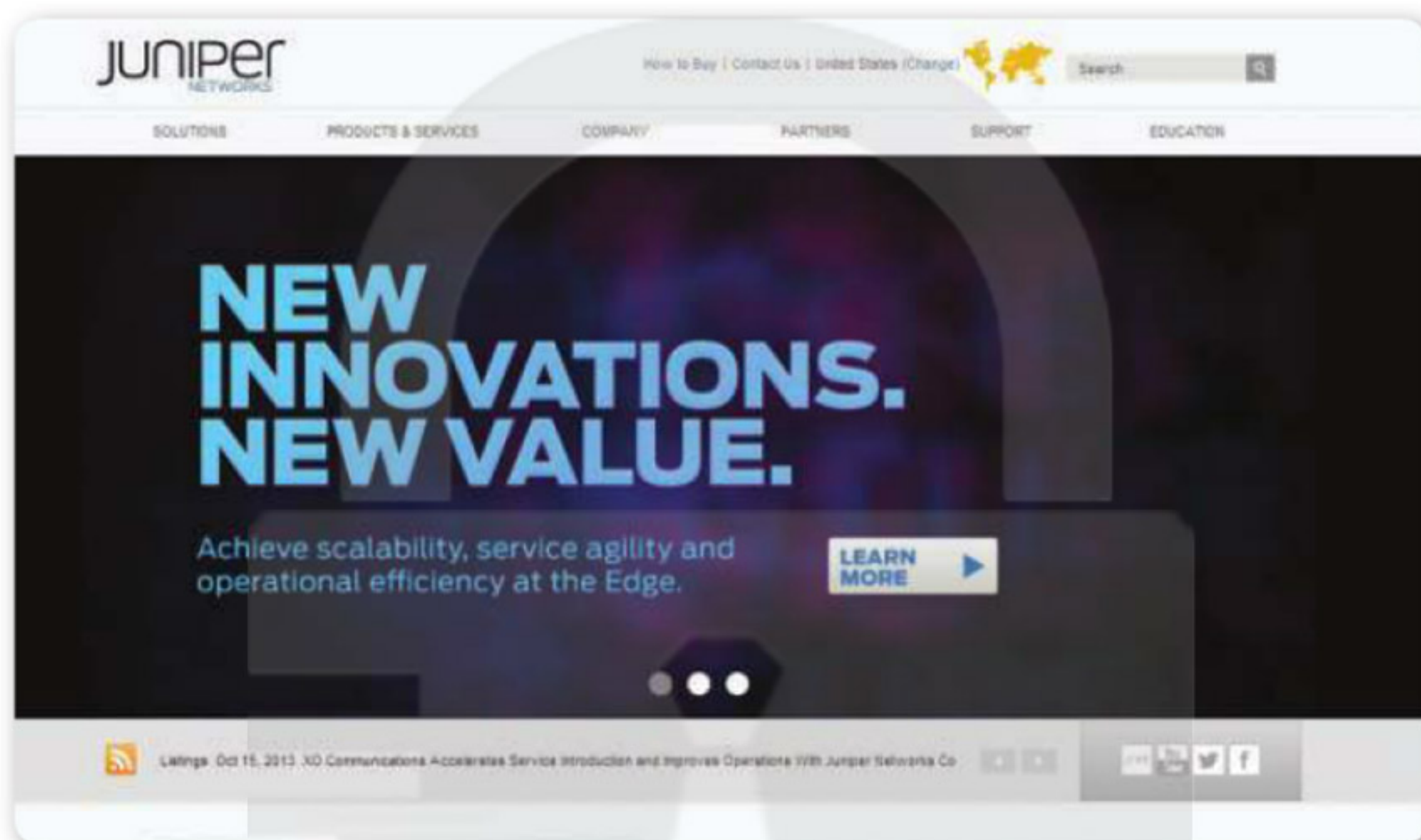


Figura 4. Juniper Networks es otro reconocido fabricante de equipos de telecomunicaciones. La empresa desarrolla su propio sistema operativo de red (**JunOS**) y cuenta con equipos de grandes prestaciones (www.juniper.net).

Port Security

Esta es una tecnología que se encuentra disponible en varios modelos de switches. Algunos permiten realizar configuraciones más personalizadas que otros, pero la mayoría ofrece lo siguiente:

- Lista blanca de MAC: permite definir qué dirección/es MAC pueden conectarse a qué puerto físico del switch. Es verdad que los usuarios avanzados podrán modificar su propia dirección MAC, pero esta es una medida de seguridad adicional muy útil.
- Lista negra de MAC: permite definir qué dirección/es no podrán conectarse nunca a la red.
- Aprender MAC: es posible definir que solamente las direcciones MAC conectadas en un momento puedan establecer conexiones, en tanto que los nuevos dispositivos estarán bloqueados.

- Configuración remota: bloquea los dispositivos que pueden administrar el equipo en forma remota.

El siguiente ejemplo para un switch Cisco configura Port Security en un puerto, definiendo la dirección MAC permitida y la acción que se tomará en caso de que se detecte una violación: deshabilitar el puerto (**shutdown**):

```
switchport port-security  
switchport port-security mac-address DIRECCION_MAC  
switchport port-security violation shutdown
```

Port Security también impide que pueda realizarse un ataque de **CAM-Overflow**, en el cual la memoria CAM del switch se llena, y este empieza a trabajar como si fuera un hub, enviando todo el tráfico a todas las interfaces. Esto permitiría que un atacante viera información confidencial.



Figura 5. Este famoso sitio mantiene una lista con un ranking de las 100 mejores herramientas de seguridad para redes (<http://sectools.org>).

DHCP Snooping

Esta tecnología permite a los switches analizar los mensajes DHCP, y aprender las asociaciones entre direcciones IP y MAC. La idea principal es que el switch permita tráfico DHCP solamente con servidores DHCP autorizados.

Este tipo de tecnología marca la nueva tendencia de los switches inteligentes, según la cual el dispositivo no solamente se limita a retransmitir paquetes, sino que también se encarga de analizar el tráfico y bloquear los ataques más comunes.

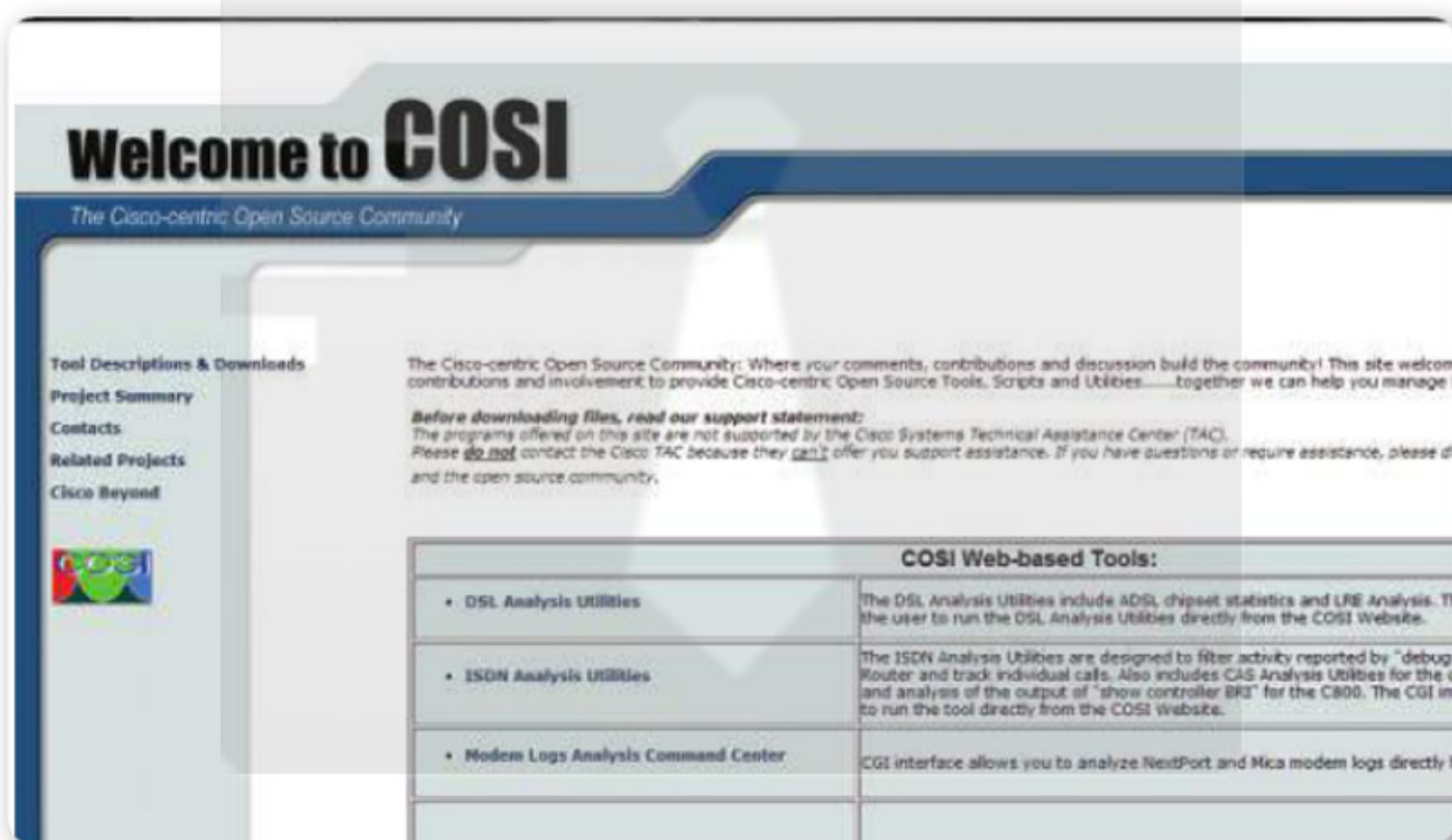


Figura 6. El sitio web **COSI** es un lugar en el que se pueden encontrar varias herramientas para trabajar con equipos Cisco (<http://cosi-nms.sourceforge.net>).

El DHCP Snooping también bloquea los ataques del tipo DHCP Starvation, en los cuales un atacante envía muchísimas peticiones DHCP con el objetivo de agotar todas las direcciones IP disponibles en el servidor.

Cuentas de acceso centralizadas

Cuando tenemos que administrar varios dispositivos, es una excelente idea centralizar nuestra base de datos de usuarios, para poder asignar

perfiles y simplificar nuestra tarea de altas, bajas y modificaciones. La siguiente configuración nos permite definir un servidor TACACS+ para autenticar a nuestros usuarios en un router Cisco:

```
aaa new-model
aaa authentication login default tacacs local
aaa authentication login consoleport none
aaa authorization network tacacs
tacacs-server host 10.6.101.101
tacacs-server key cisco
```

Esto nos será de utilidad no solo para nuestros dispositivos de telecomunicaciones, sino también para todos nuestros servidores y otros equipos que requieran ser gestionados, y para los cuales podemos elegir entre varias tecnologías de control de acceso. Detallamos algunas de ellas a continuación.

TACACS+

Es un protocolo desarrollado por Cisco, que nos provee de autenticación, autorización y registros (en inglés, las siglas AAA). Utiliza el protocolo



MEJORES PRÁCTICAS



En Internet hay disponible una gran cantidad de documentos con mejores prácticas de seguridad. Debemos ser cuidadosos acerca de las fuentes de información que utilizamos y verificar que las configuraciones funcionen bien en un ambiente de pruebas antes de llevarlas a un ambiente productivo. Algunos de los documentos mejor redactados y más confiables son los desarrollados por la **National Security Agency** o **NSA** (www.nsa.gov).

lo TCP para el intercambio de datos. El tráfico es encriptado para brindar mayor seguridad a las comunicaciones entre los clientes y el servidor.

Podemos encontrar un servidor de TACACS+ de código abierto en el sitio **www.shrubbery.net/tac_plus**.

Radius

A diferencia de **TACACS+**, **Radius** utiliza el protocolo UDP para el intercambio de datos, y unifica los procesos de autenticación y autorización, lo cual presenta desventajas. Pero sigue siendo una buena alternativa. En **<http://freeradius.org>** podemos encontrar un servidor Radius de código abierto. Además, Microsoft Active Directory puede ser configurado para brindar servicios de Radius utilizando su base de datos de usuarios.

Diameter

Este protocolo es el sucesor de Radius, y cuenta con grandes ventajas, tanto sobre su predecesor como sobre TACACS+. Está encriptado con TLS, permite notificar errores, soporta servicios con roaming y es extensible para poder agregarle nuevas funcionalidades. Podemos encontrar un servidor Diameter de código abierto en **www.freediameter.net**.

Utilización de servidores syslog

Una de las formas de contar con un registro de todo lo que sucede en nuestros equipos de telecomunicaciones es definir un servidor de syslog para que todos los logs sean enviados a él. Estos parámetros podemos definirlos en un router o switch de la empresa Cisco, aunque la gran mayoría de este tipo de dispositivos, de cualquier fabricante, permite estas configuraciones. Además, es muy sencillo configurar un servidor syslog en cualquier sistema del tipo Unix. Con los siguientes comandos podemos definir en un router o switch Cisco a qué servidor syslog le vamos a enviar los logs:


```
logging IP_o_Hostname
logging facility local7
logging on
```



Firewalls

El concepto de firewall ha cambiado mucho en los últimos años, y ha dejado de ser algo tan simple como filtrado por origen, destino y puertos, para pasar a abarcar equipos o aplicaciones muchísimo más granulares, de modo que, incluso, llegan a inspeccionar el contenido de los paquetes que pasan a través de ellos e interpretan los protocolos utilizados para la comunicación. Es por eso que debemos aprovechar al máximo estas nuevas capacidades, para incluirlas dentro de nuestras medidas de protección.

EL FIREWALL LLEGA
A INSPECCIONAR
EL CONTENIDO DE
LOS PAQUETES
TRANSMITIDOS



Es preciso tener en cuenta si vamos a seleccionar un dispositivo del tipo UTM (*Unified Threat Management*), que contiene varias capacidades en un mismo equipo, como antivirus, antispam, filtrado web, y muchas otras; o si vamos a optar por instalar un equipo para cada función importante. Esta es una de las cuestiones que se nos puede presentar al llevar a cabo la tarea de diseñar las medidas de protección para una red. La decisión que tomemos deberá estar basada en nuestras necesidades. Por ejemplo, en caso de que precisemos capacidades avanzadas de filtrado antispam, y vayamos a manejar una cantidad muy grande de correos electrónicos, será recomendable contar con un dispositivo dedicado a estas tareas.

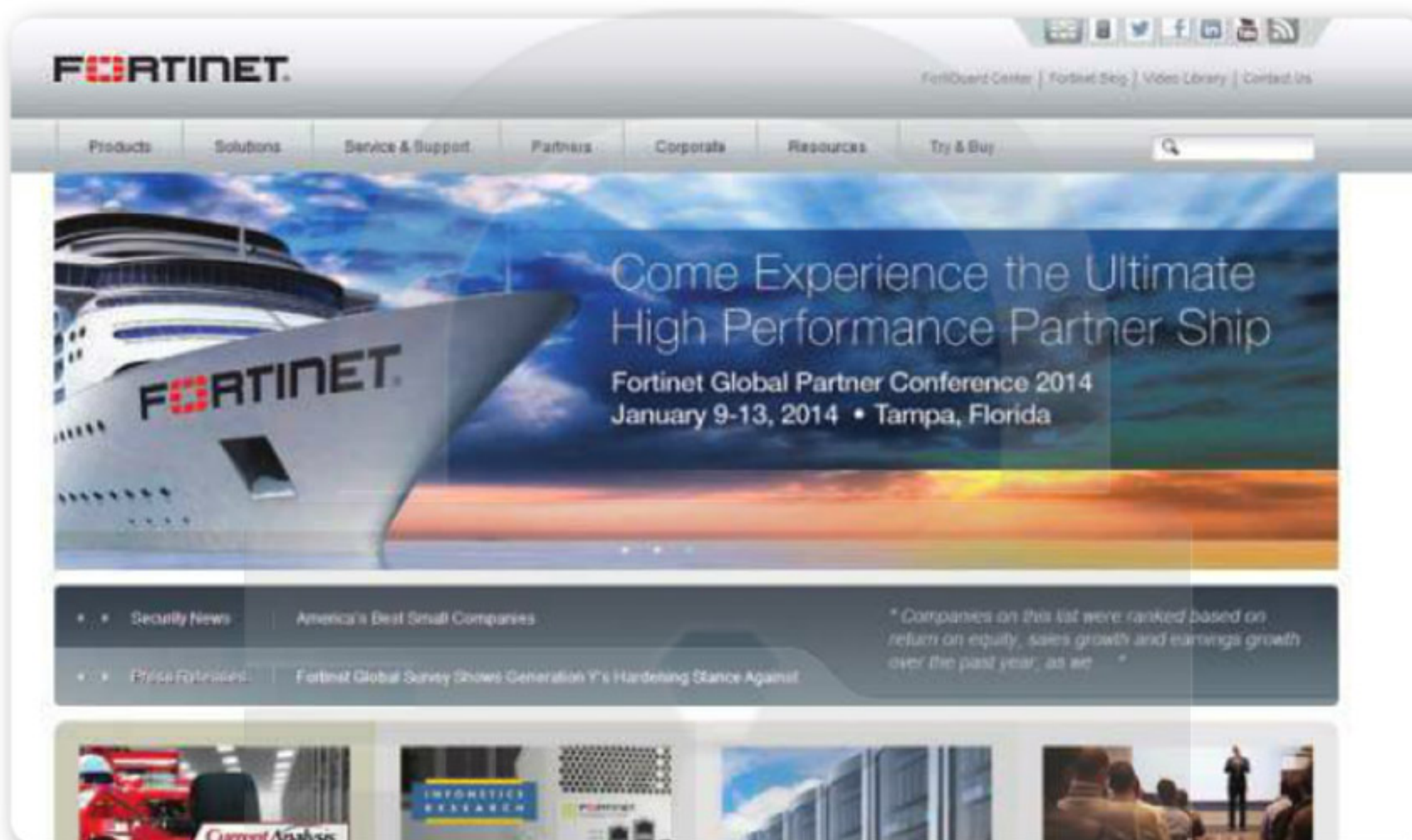


Figura 7. Fortinet es un fabricante de dispositivos de seguridad que cuenta con una gran reputación, y una muy buena relación de calidad y precio (www.fortinet.com).

En cuanto a la selección del firewall que vamos a implementar, si bien muchos nuevos productos ofrecen muchísimas capacidades, el filtrado por origen, destino y puertos bloquea la mayor parte de los ataques y



ALTERNATIVAS DE CÓDIGO ABIERTO



Si no podemos contar con un appliance de seguridad, podemos optar por instalar algunas de las alternativas de código abierto, que han demostrado ser excelentes productos. Muchas de ellas ofrecen versiones pagas, que incluyen funciones adicionales. Algunos ejemplos son: **m0n0wall** (<http://m0n0.ch>), **IPCop** (www.ipcop.org) y **Untangle** (www.untangle.com). Para consultar una lista más completa y detallada, podemos visitar: http://en.wikipedia.org/wiki/List_of_router_or_firewall_distributions.



accesos malintencionados. Debemos considerar las otras características como adicionales, y evaluar si verdaderamente sacaremos provecho de ellas. Cabe destacar que, a mayor cantidad de características, mayor será la dificultad de administración y mantenimiento, además de que mayor será la probabilidad de que se presenten fallas en el dispositivo.

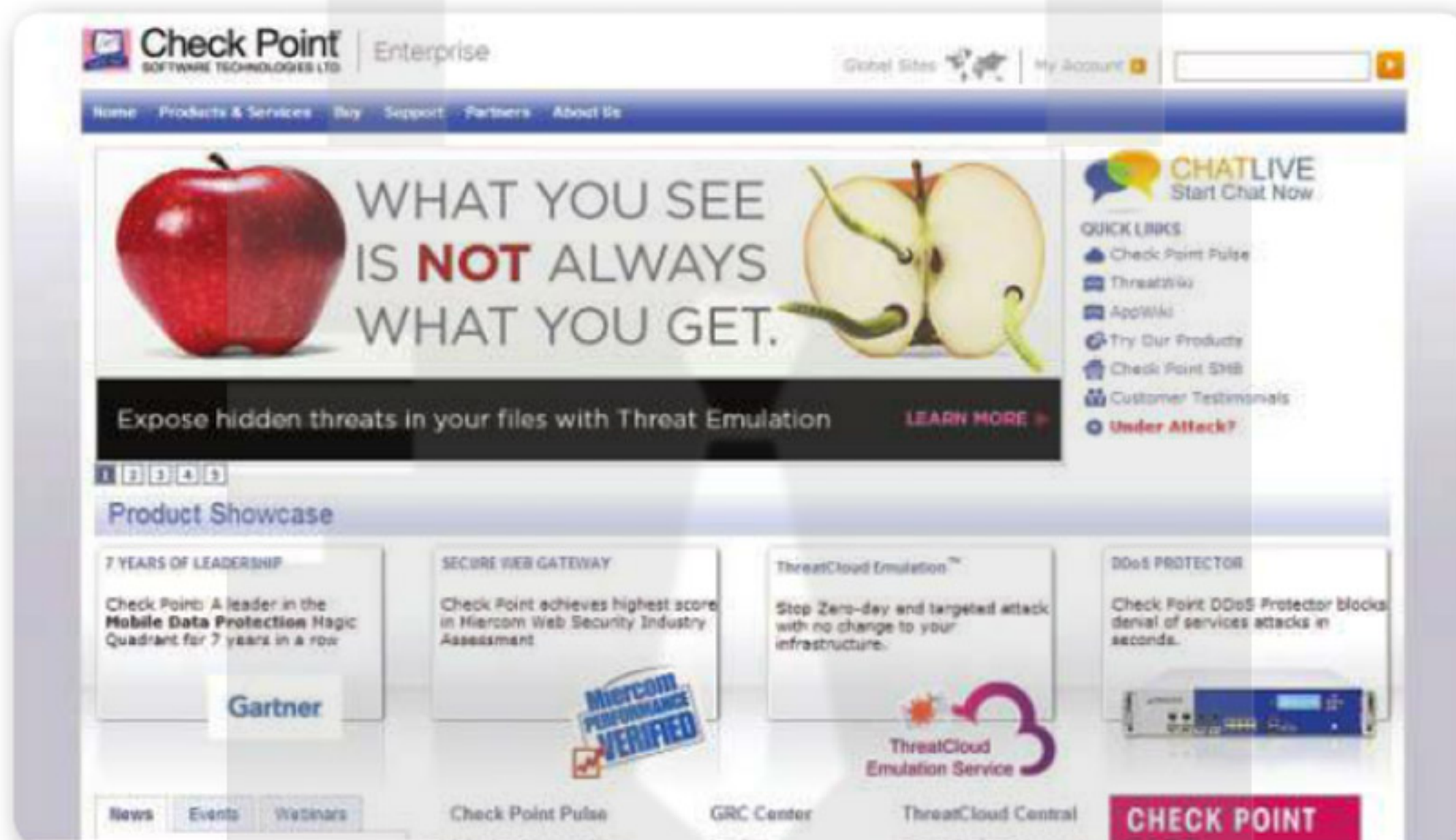


Figura 8. Checkpoint es uno de los fabricantes de dispositivos de tipo firewall más destacados en el mundo. Cuenta con excelentes productos y siempre es pionero en agregar nuevas características a sus equipos (www.checkpoint.com).

Al crear reglas de filtrado, es de suma importancia que lo hagamos de la forma más específica posible. Por ejemplo, si debemos permitir que un equipo acceda a una aplicación remota, debemos permitir que solo ese equipo acceda únicamente a las direcciones y puertos que se van a utilizar para dicha aplicación, ni más ni menos.

En caso de que no contemos con los recursos económicos para adquirir un dispositivo preparado específicamente para trabajar como un firewall, podemos utilizar un router o un servidor con alguna distribución de GNU/Linux o BSD. Las ventajas y desventajas de cada una de estas opciones se explican en el apartado “Diseño de redes seguras”.



Redes inalámbricas

Una de las comodidades tecnológicas requeridas en muchas organizaciones son las redes inalámbricas, que simplifican las conexiones al evitar la presencia de cables, aunque también aumentan el campo de conexión disponible para las personas malintencionadas.

Name	BSSID	T	C	Ch	Freq	Pkts	Size	Bcr%	Sig	Clnt	Manuf	City	Seen By
TRENDnet	00:14:D1:5F:97:12	A	0	1	2417	1	0B	---	---	1	TrendwareI	---	wlan0
QqF93	00:1F:90:F2:CB:C2	A	N	1	2412	1	0B	---	---	1	ActiontecE	US	wlan0
landscapers	00:14:BF:07:2F:84	A	N	6	2437	2	0B	10%	-86	1	Cisco-Link	---	wlan0
linksys_SES_45997	00:16:B6:1B:E4:FF	A	0	6	2447	2	0B	---	---	1	Cisco-Link	---	wlan0
linksys	00:1A:70:D9:BC:13	A	N	6	2437	2	0B	---	---	1	Cisco-Link	---	wlan0
MPA41	00:1F:90:E6:E0:84	A	N	11	2462	3	0B	---	---	1	ActiontecE	---	wlan0
TFS	00:09:5B:07:9D:B2	A	N	---	2462	4	0B	---	---	1	Netgear	---	wlan0
Autogroup Probe	00:13:E8:92:3F:CB	P	N	---	---	5	0B	---	0	1	IntelCorpo	---	wlan0
meskas	00:18:01:F5:65:E1	A	0	11	2462	7	0B	10%	-87	1	ActiontecE	US	wlan0
ES103	00:1F:90:FA:F4:C8	A	N	---	2412	8	0B	---	---	1	ActiontecE	---	wlan0
Xu Chen	00:18:01:F9:70:F0	A	N	6	2442	9	0B	0%	-75	1	ActiontecE	US	wlan0
7J480	00:1F:90:E6:D4:F1	A	N	11	2462	14	0B	---	-70	1	ActiontecE	---	wlan0
TK421	00:18:01:FE:68:77	A	0	6	2437	14	0B	---	-82	1	ActiontecE	---	wlan0
Elina-PC-Wireless	00:24:B2:0E:E6:E2	A	0	11	2462	14	0B	0%	-31	1	Netgear	---	wlan0
Pickles	00:1F:33:F3:C5:4A	A	0	2	2422	17	0B	---	---	1	Netgear	---	wlan0
3Bc8	00:16:CE:07:60:77	A	N	6	2447	38	0B	---	-76	1	HorvatiPrec	---	wlan0

MAC	Crypt	Freq	Pkts	Size	Manuf	DHCP Host	DHCP OS
00:13:10:35:59:CB	0	2462	624	0B	Cisco-Link	---	---
00:11:24:A4:6F:B3	6	2452	6	708B	AppleCompu	---	---
00:13:10:35:59:C9	5	2452	5	1K	Cisco-Link	---	---
00:17:AB:3D:25:9B	4	2452	4	626B	Nintendo	---	---
00:13:E8:92:3F:CB	8	----	8	1K	IntelCorpo	---	---

Figura 9. Kismet es una herramienta de código abierto que nos permite detectar las redes inalámbricas existentes y capturar su tráfico (www.kismetwireless.net).



REDES INALÁMBRICAS

Debemos visualizar las redes inalámbricas como un tipo de red más, y dejar atrás el viejo mito de que utilizarlas significa hacer que nuestra red se vuelva totalmente vulnerable. Siempre tenemos que estar abiertos a implementar este tipo de conexiones, porque actualmente son necesarias para el buen funcionamiento de la mayoría de las organizaciones.

A diferencia de lo que muchas veces se cree, las redes inalámbricas pueden tener una muy buena seguridad, si se las configura correctamente. Las creencias de inseguridad en este tipo de redes se fundamentan, principalmente, en que los primeros protocolos de conexión no eran robustos y presentaban fallas que volvían muy fácil el ataque. En la actualidad, los protocolos se han mejorado y brindan excelentes características de seguridad.

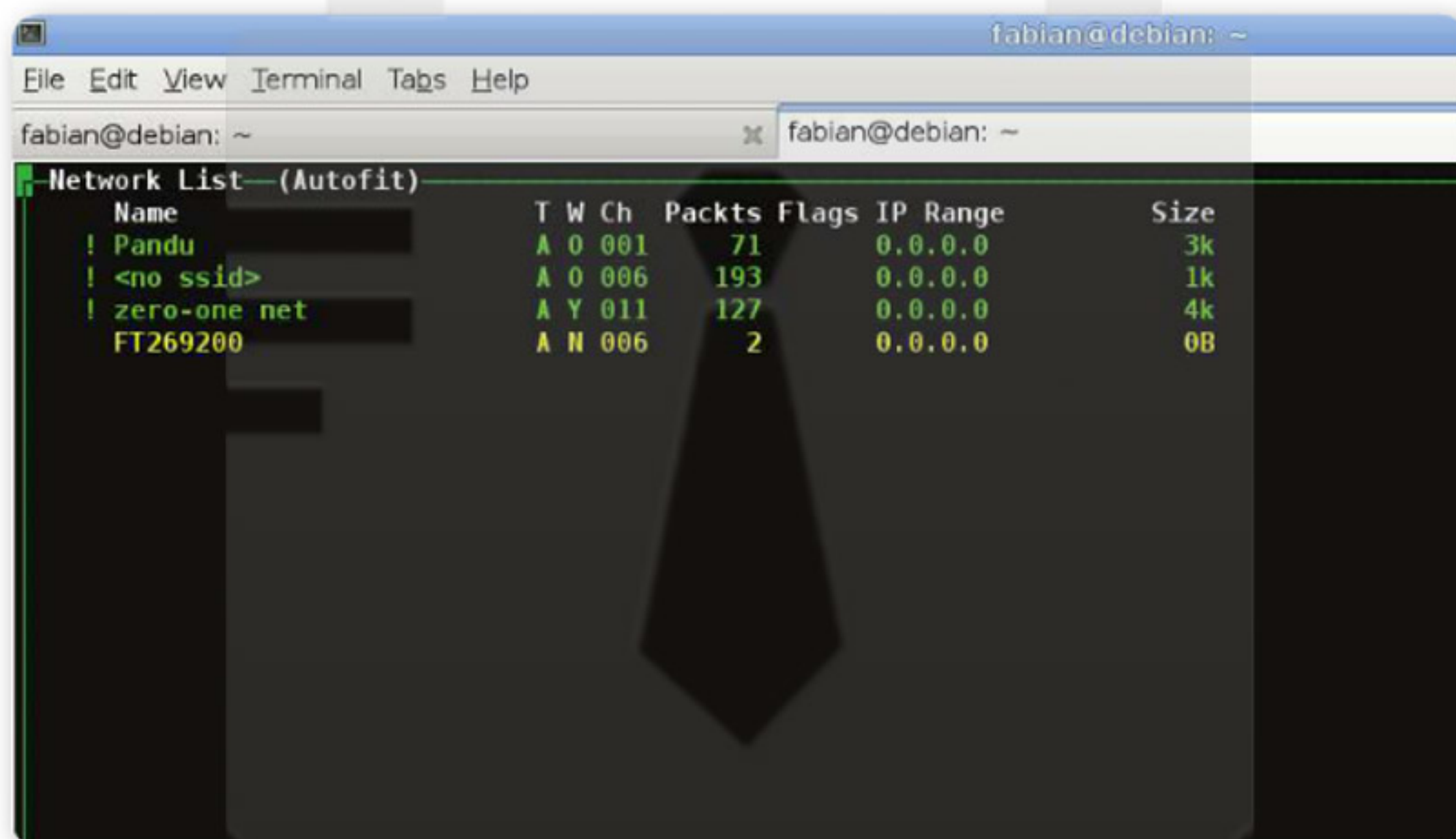


Figura 10. Aquí podemos ver cómo utilizamos la herramienta **Kismet** para conocer rápidamente cuáles son las redes inalámbricas que están a nuestro alcance. Hecho esto, podemos analizar más a fondo la configuración de cada una de ellas.

Todas las vulnerabilidades que existen en las redes cableadas se aplican a las redes inalámbricas. Pero esto no funciona a la inversa, porque las redes inalámbricas presentan nuevos riesgos, al tener un medio de transmisión compartido por todos. Cualquier información que circule por la red sin ser encriptada, puede ser fácilmente capturada por una persona que esté relativamente cerca de los dispositivos que transmiten y reciben los datos. Es por eso que debemos tener algunas consideraciones especiales, que podemos ver en la siguiente lista:



Figura 11. FlukeNetworks ofrece una gran cantidad de productos para el análisis de redes inalámbricas. Desde software instalable en una PC, hasta un dispositivo del tipo tablet desarrollado particularmente para analizar este tipo de redes (www.flukenetworks.com).

- **Modificar los SSID que vienen por defecto:** generalmente, los SSID que vienen por defecto brindan información acerca del punto de acceso que podría ser utilizado por un atacante para buscar vulnerabilidades en la red inalámbrica.
- **No publicar el SSID en modo broadcast:** esto hará que nuestra red no sea tan visible, aunque puede ser encontrada por programas especializados en detección de redes inalámbricas.
- **Modificar periódicamente las claves precompartidas:** hará más difícil la tarea de crackear las claves, porque le dará menos tiempo al atacante para hallar la clave correcta.
- **Implementar métodos de autenticación fuerte:** contando con servidores LDAP o Radius para la autenticación, nos permitirá identificar fácilmente al usuario que está conectado a la red. También podemos utilizar smart cards y tokens.

- **Utilizar WPA/WPA2 en lugar de WEP:** es ampliamente conocido que la seguridad que ofrece el protocolo WEP es casi nula. WPA y WPA2 brindan una mejor seguridad.
- **Implementar las últimas medidas disponibles:** este tipo de tecnologías evoluciona constantemente, así que debemos estar al tanto de las nuevas capacidades que brindan nuestros equipos.

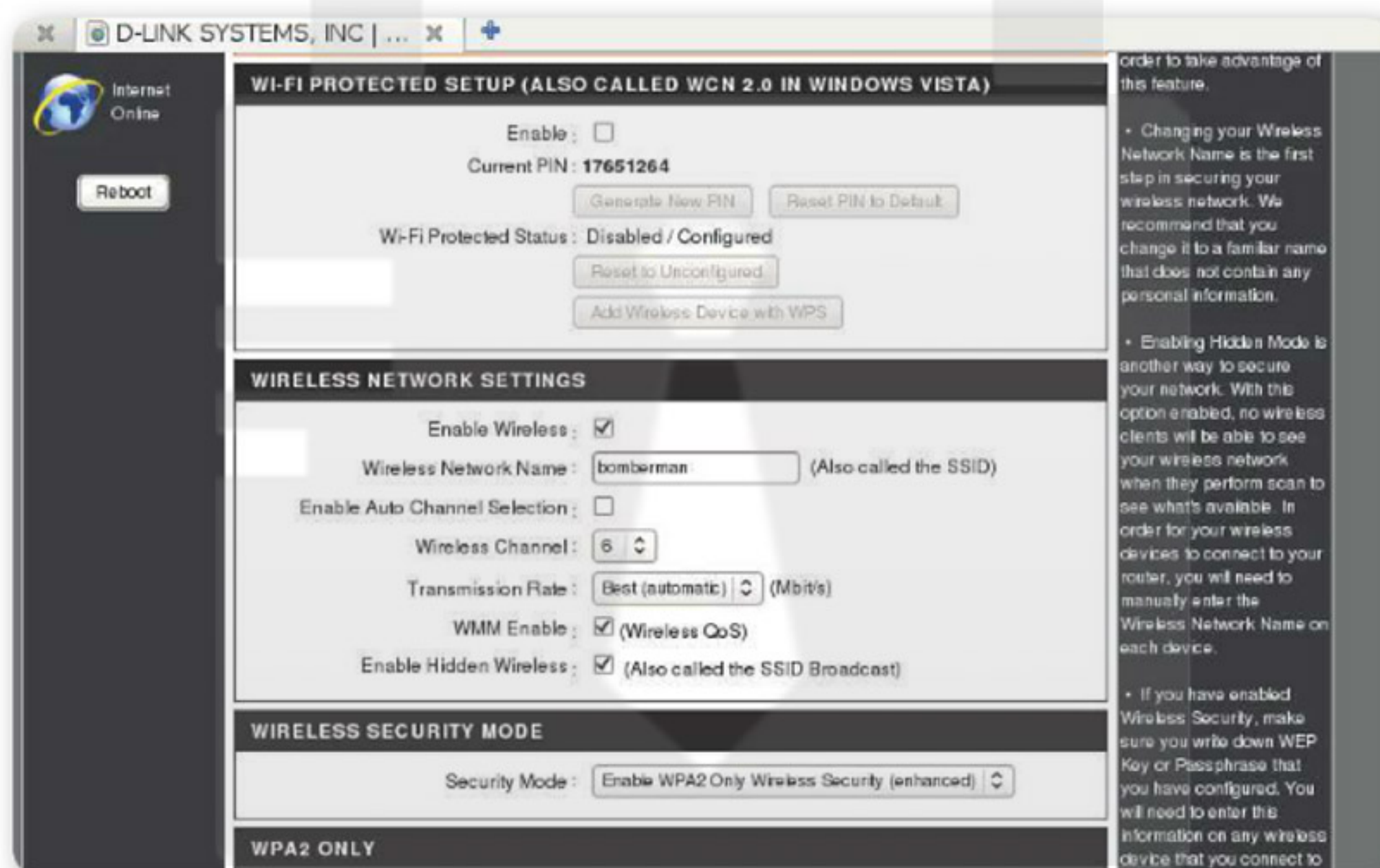


Figura 12. En la captura de pantalla podemos ver cómo se encuentran configuradas algunas de las opciones de seguridad de la red inalámbrica en un **router D-Link DIR-300**. Algunas son **WPA2**, **SSID oculto**, el **cifrado de tráfico** y el **protocolo PSK**.

Como podemos observar, muchas de estas medidas simplemente complican un poco la tarea de un atacante en su camino al éxito de romper la seguridad de una red. Es por eso que debemos seleccionar cuidadosamente las configuraciones por implementar, manteniendo un buen balance entre la seguridad y la usabilidad de la red. También es importante analizar periódicamente nuestra red en busca de dispositivos sospechosos o configuraciones débiles.


```

Home - PuTTY

Aircrack-ng 1.0

[00:00:18] Tested 1514 keys (got 30566 IVs)

KB    depth  byte(vote)
0     0/ 9    1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
1     7/ 9    64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
2     0/ 1    1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
3     0/ 3    1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
4     0/ 7    1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)

KEY FOUND! [ 1F:1F:1F:1F:1F ]
Decrypted correctly: 100%

~$ █

```

Figura 13. Aircrack es un software de código abierto utilizado para romper la seguridad de redes **WEP** y **WPA** (www.aircrack-ng.org).



Prevención de intrusos

Una de las tecnologías más avanzadas para proteger nuestras redes es la detección y prevención de intrusos, que nos permite trabajar de



ROUTERS INALÁMBRICOS



Es habitual que los empleados conecten routers inalámbricos a la red cableada, con el objetivo de utilizar sus smartphones o PDAs. Al hacer esto, no suelen tener los recaudos de seguridad necesarios, y el resultado es una red inalámbrica insegura, que podría servir como puente para acceder a los recursos de la red de área local.



forma inteligente, analizando el tráfico y bloqueando los ataques automáticamente. Estos sistemas son complejos y puede llevar un tiempo configurarlos, pero son capaces de brindarnos un excelente nivel de seguridad al trabajar de forma automatizada y proactiva. La decisión de instalar o no este tipo de soluciones dependerá de la complejidad de la red, nuestros recursos y necesidades.

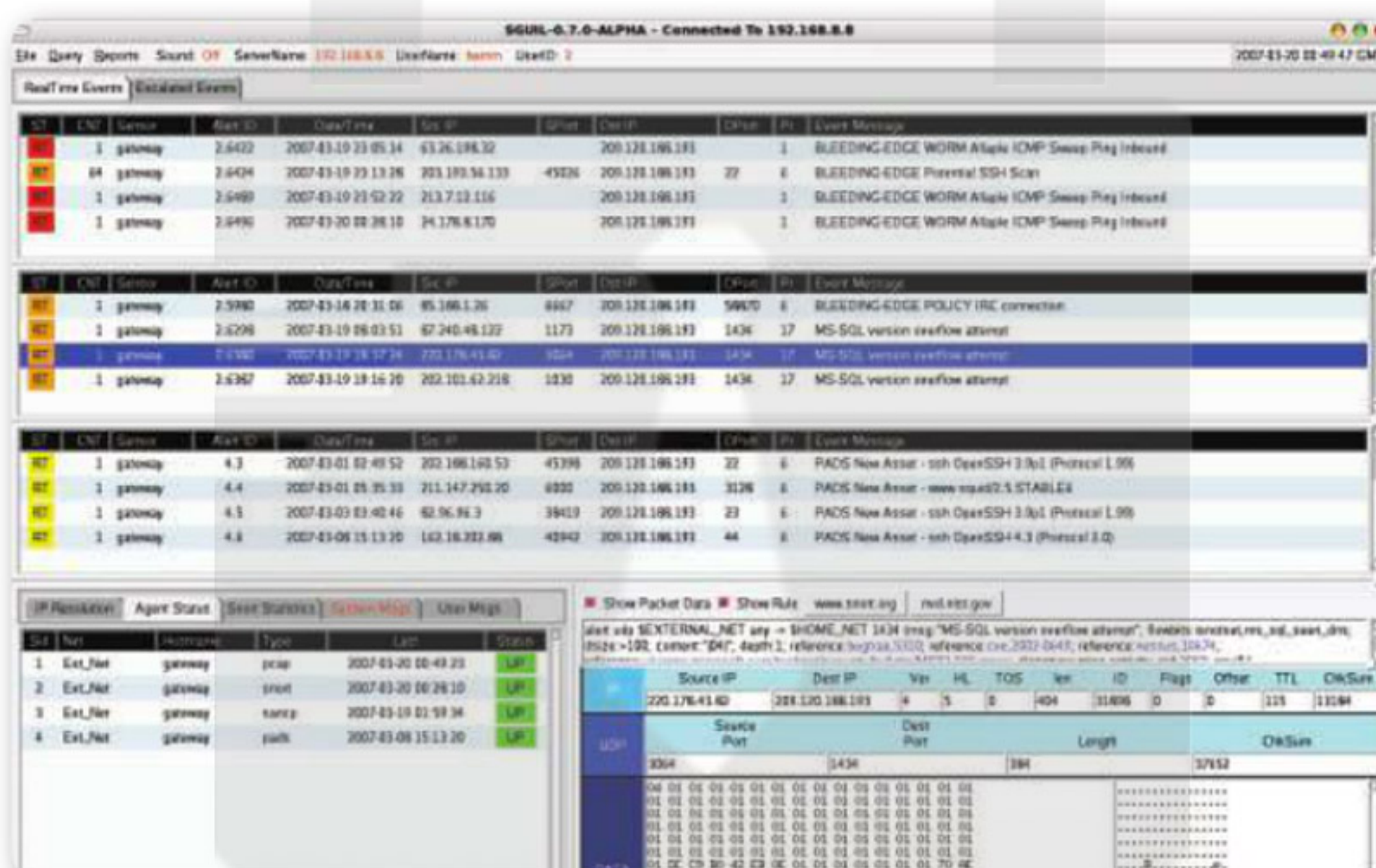


Figura 14. Snort es el IDS de código abierto más reconocido. Cuenta con varios años de desarrollo y excelentes capacidades de detección. En la imagen podemos observar cómo se utiliza la interfaz Sguil para interpretar las alertas de Snort (www.snort.org).

Los sistemas que solo pueden detectar ataques se conocen como **Sistemas de Detección de Intrusos (IDS)**, y los que pueden tomar acciones para bloquear estos ataques se llaman **Sistemas de Prevención de Intrusos (IPS)**. Obviamente, los IPS son bastante más complejos que los IDS, y requieren de mayor atención al configurarse, porque pueden bloquear tráfico legítimo e impactar negativamente en la operatoria de la organización. Es común referirse a ambos tipos de sistemas, simplemente, como IDS, y así lo haremos a lo largo del libro.

Muchos IPS permiten trabajar temporalmente como si fueran IDS, solo notificando los ataques detectados, lo que nos da la oportunidad de visualizar cómo funciona la solución y configurarla correctamente, para luego habilitar las capacidades de bloqueo. Esto es algo recomendable para iniciarnos en la configuración y puesta a punto de este tipo de sistemas.

Los IDS pueden estar basados en host (HIDS), que se instalan en un servidor para analizar el tráfico y las acciones realizadas dentro de él, para detectar ataques, los cuales analizaremos en el siguiente capítulo. También pueden estar basados en red (NIDS), que se utilizan para analizar el tráfico de toda la red en busca de ataques entre dispositivos.

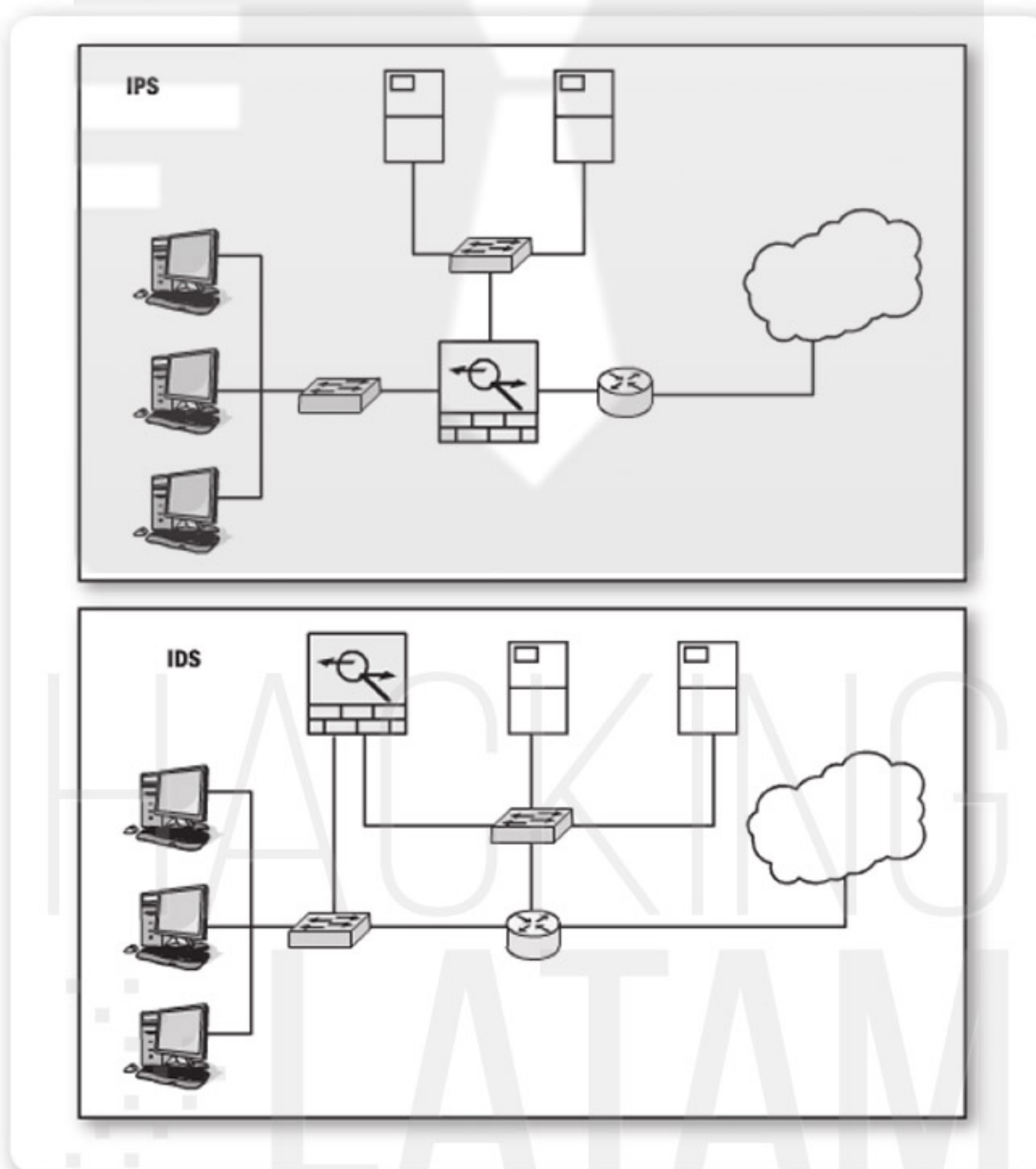


Figura 15. En el diagrama podemos observar cómo un dispositivo IPS se ubica de modo tal que puede bloquear conexiones y controlar, así, el paso del tráfico.



Desde el punto de vista del funcionamiento, un IDS puede verse, simplemente, como un analizador que reconoce distintos patrones de ataque, ya sea analizando un archivo de logs, un comportamiento del sistema operativo o las características de los paquetes enviados de un host a otro.



Figura 16. Suricata es un IDS de código abierto desarrollado por la **Open Information Security Foundation**, que implementa novedosas tecnologías de detección (www.openinfosecfoundation.org).



PRELUDE

Debemos prestar atención a las nuevas tendencias acerca de este tipo de tecnologías. Existen sistemas como **Prelude** (www.prelude-technologies.com) que se llaman **IDS híbridos** y cuentan con capacidades para detectar intrusiones analizando varias fuentes de información al mismo tiempo y relacionándolas. Estos productos son algo así como una mezcla entre los IDS y los SIEM.

En la selección de un IDS debemos tener en cuenta, particularmente, las capacidades de detección y bloqueo de ataques, la facilidad de configuración y las capacidades de monitoreo. Esto se debe a que, muchas veces, nos será más conveniente seleccionar una solución simple y sencilla que una mucho más compleja, aunque la segunda tenga más características que la primera.



Implementación de sistemas IDS

Una de las consideraciones más importantes a tener en cuenta antes de implementar un sistema de este tipo, es determinar si verdaderamente lo necesitamos y si vamos a poder contar con los recursos humanos necesarios para poder administrarlo.

Una vez decidida la implementación, debemos seleccionar un producto, teniendo en cuenta particularmente cuáles son las características y la complejidad del mismo, para determinar si es lo que se ajusta a nuestras necesidades.

Este tipo de sistemas suele tener un costo elevado, por lo que es recomendable realizar una primera aproximación a través de algún proyecto de código abierto (Snort puede ser la opción más viable). Una vez que hayamos realizado dichas pruebas, estaremos en una mejor posición para decidir si necesitamos este tipo de sistemas y si vale la pena optar por una opción comercial, o si nuestras necesidades son cubiertas con el producto gratuito.

Cualquiera sea la decisión, tengamos en cuenta que un sistema IDS puede facilitarnos todas nuestras tareas, y que podría ser una decisión inteligente asignar muchos recursos a instalar y mantener esta solución.



Administración remota

Una de las características más utilizadas por los administradores de red para simplificar su trabajo diario es el manejo remoto de los equipos de telecomunicaciones, lo que permite gestionar toda una red desde la como-



didad de una única terminal. Este tipo de protocolos y herramientas son necesarios, pero deben ser utilizados y configurados con cuidado, porque suelen estar dentro de los principales intereses de una persona malintencionada que busque atacar nuestra red.

Dependiendo del fabricante, cada dispositivo puede contar con varias interfaces de administración, como SNMP, SSH, interfaces web y protocolos propietarios. Es de suma importancia que utilicemos solamente protocolos que encripten el tráfico, como SNMPv3, SSH y HTTPS. Además, debemos tener los recaudos necesarios acerca de la fortaleza de las contraseñas por utilizar.

De ser posible, es recomendable seleccionar un método de gestión que nos permita automatizar tareas de rutina, como lo son las copias de seguridad de configuraciones. Varios fabricantes cuentan con herramientas propias, que suelen limitarse a gestionar sus equipos.

Debemos considerar que existen soluciones en el mercado compatibles con varios fabricantes. Si optamos por utilizar herramientas multifabricante, debemos verificar que sean soportados todos los equipos presentes en la infraestructura.

En el caso de los dispositivos Cisco, es recomendable habilitar la administración exclusivamente por SSH versión 2, bloqueando tanto la versión 1 de este protocolo así como el protocolo Telnet. Abajo vemos un ejemplo de cómo realizar esto:

```
crypto key generate rsa
ip ssh version 2
ip ssh authentication-retries 3
ip ssh logging events

line vty 0 4
transport input ssh
```


Con la siguiente configuración establecemos:

1. Generar las claves RSA para utilizar con SSH.
2. Utilizar solamente la versión 2 de SSH.
3. Permitir solamente tres intentos fallidos de conexión.
4. Guardar el registro de eventos de SSH.
5. Configurar las líneas vty 0-4.
6. Aceptar administración solo por SSH (bloquea Telnet).

Al habilitar usuarios para poder acceder a los dispositivos y gestionarlos, es necesario tener en cuenta la implementación de permisos y perfiles, para que cada uno pueda acceder solo a las funciones que necesita para realizar sus tareas diarias. También es de suma importancia guardar un registro de todas las acciones realizadas sobre los equipos, de modo de poder analizar posteriormente cualquier anomalía o cambio de configuración no autorizado.

Diff for /UL/configs/141.211.43.119 between versions 1.44 and 1.45	
version 1.44, 2005-10-24 17:20:24	version 1.45, 2005-10-24 22:20:24
Line 33	Line 33
!BootFlash: Standby is not up.	!BootFlash: Standby is not up.
!	!
!Flash: nvram: Directory of nvram:/	!Flash: nvram: Directory of nvram:/
!Flash: nvram: 1918 -rw- 18001 <no date> startup-config	!Flash: nvram: 1918 -rw- 18060 <no date> startup-config
!Flash: nvram: 1919 --- 3596 <no date> private-config	!Flash: nvram: 1919 --- 3596 <no date> private-config
!Flash: nvram: 1920 -rw- 18001 <no date> underlying-config	!Flash: nvram: 1920 -rw- 18060 <no date> underlying-config
!Flash: nvram: 1 --- 4 <no date> if_cold_start	!Flash: nvram: 1 --- 4 <no date> if_cold_start
!Flash: nvram: 2 --- 20 <no date> persistent-data	!Flash: nvram: 2 --- 20 <no date> persistent-data
!Flash: nvram: 3 -rw- 0 <no date> ifindex-table	!Flash: nvram: 3 -rw- 0 <no date> ifindex-table
!Flash: nvram: 1964024 bytes total (1939333 bytes free)	!Flash: nvram: 1964024 bytes total (1939274 bytes free)
!	!
!Flash: bootflash: Directory of bootflash:/	!Flash: bootflash: Directory of bootflash:/
!Flash: bootflash: No files in directory	!Flash: bootflash: No files in directory
Line 863 ip access-list extended MSDP-filter	Line 863 ip access-list extended MSDP-filter
logging source-interface Loopback0	logging source-interface Loopback0
logging 131.215.207.45	logging 131.215.207.45
logging 141.211.43.109	logging 141.211.43.109
!	!
route-map Abilene-in-IGRD-Demo permit 10	route-map Abilene-in-IGRD-Demo permit 10
match ip address match-all IGRD-in-Abilene	match ip address match-all IGRD-in-Abilene
Line 874 route-map Abilene-out-IGRD-Demo permit	Line 875 route-map Abilene-out-IGRD-Demo permit
!	!
snmp-server community physcitt RO	snmp-server community physcitt RO
snmp-server community ultralight RO	snmp-server community ultralight RO
!	!
snmp-server location Randall rm 2268	snmp-server location Randall rm 2268
snmp-server contact Shawn McKee, smckee@umich.edu 734-764-4395	snmp-server contact Shawn McKee, smckee@umich.edu 734-764-4395
tacacs-server host 141.211.147.47	tacacs-server host 141.211.147.47

Figura 17. El software de código abierto **RANCID** nos permite descargar automáticamente la configuración de nuestros dispositivos y almacenar un historial de versiones, que muestra las diferencias entre una y otra (www.shrubby.net/rancid).

CLI vs. TUI vs. GUI vs. WUI

Existen varias formas de interactuar con un dispositivo o sistema. Hace muchos años, la única manera disponible era a través de la línea de comandos o CLI (*Command Line Interface*). Con el correr del tiempo, se fueron desarrollando las TUI (*Text User Interface*), que, básicamente, son interfaces de texto un poco más amigables, con menús y ayuda por pantalla. Con la gran explosión de los entornos de escritorio, vinieron las GUI (*Graphic User Interface*), que presentaban ventanas, botones y nuevos componentes que hacen más fácil la interacción para el usuario. En los últimos años se han puesto muy de moda las WUI (*Web User Interface*), muy similares a las GUI, pero a las que se accede a través de un servidor web.



Figura 18. ASDM es una herramienta desarrollada por Cisco, que ofrece la capacidad de gestionar sus dispositivos de seguridad. El cliente se ejecuta sobre plataformas Microsoft Windows.

Hecha esta pequeña diferenciación de términos, podemos decir que, actualmente, en el caso de los sistemas que están pensados para ser accedidos por personas con altos conocimientos tecnológicos, aún predominan

las interfaces por línea de comandos. Si bien es cierto que la mayoría de dichos sistemas cuenta con GUI o WUI, estas no ofrecen la misma cantidad de opciones que las CLI. Por ejemplo, en los routers y firewalls, es muy común que las opciones más importantes y de uso frecuente estén disponibles dentro de la configuración por interfaz gráfica, pero existe un número de opciones avanzadas y de uso no muy frecuente que solo pueden ser accedidas a través de la línea de comandos. Por lo tanto, es ampliamente recomendable que nos familiaricemos con este tipo de interfaces. Aunque no vayamos a utilizarlas en nuestras tareas diarias, además de presentar opciones que no están disponibles a través de otras interfaces, suelen estar disponibles siempre, porque son muy simples. Por el contrario, las interfaces GUI y WUI pueden ser inaccesibles en ciertas circunstancias.



Figura 19. IBM Tivoli es un software avanzado que permite gestionar nuestros dispositivos de telecomunicaciones, servidores y otro tipo de equipamiento (www.ibm.com).

Por último, otra de las grandes ventajas de las **CLI** es que nos permiten automatizar tareas fácilmente, a través de lenguajes de **scripting** como

Python, Perl y Ruby. Esto nos permitirá, por ejemplo, realizar funciones de backup, reportes o tareas de mantenimiento de forma programada y sin interacción del personal.

Protocolos TCP/IP

Además de los protocolos IP, TCP, UDP e ICMP, la suite de protocolos TCP/IP contiene otros componentes fundamentales en las arquitecturas de red de todo el mundo. Es por eso que debemos prestarles especial atención y conocerlos a fondo si pretendemos ser verdaderos profesionales de la seguridad.

Algunos de los protocolos que seguramente utilizamos dentro de nuestra organización son DHCP, DNS, SSH, HTTP, FTP, SMTP, POP3, IMAP, SNMP y SSL/TLS. A continuación, analizaremos cada uno de ellos.

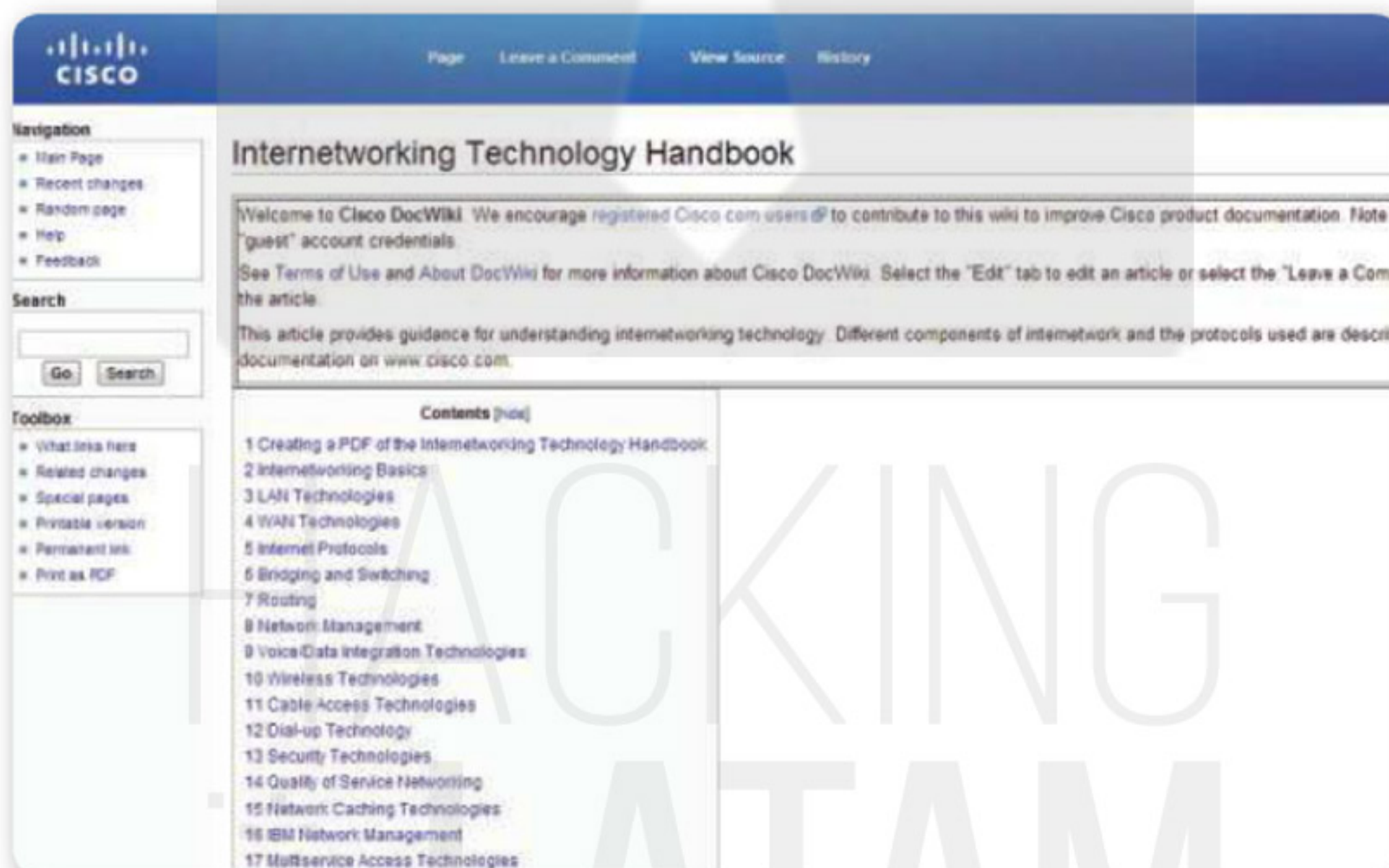


Figura 20. El sitio wiki de **Cisco** alberga un interesante documento llamado **Internetworking Technology Handbook**, que explica los protocolos relacionados con las redes y su funcionamiento (http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook).

SSH

Secure Shell es el nombre tanto del protocolo como del programa que lo implementa, y sirve para acceder a los dispositivos a través de la red. Es un reemplazo para el protocolo Telnet, que presentaba varias vulnerabilidades. Además, cuenta con diversas capacidades avanzadas, como copiar archivos y redirigir el tráfico a otras aplicaciones, para crear un túnel seguro.

Es muy habitual usarlo para acceder a servidores UNIX y dispositivos de red como routers, switches y firewalls. La versión recomendada es la 2, porque la 1 presenta algunas vulnerabilidades graves.

Es de suma utilidad saber utilizar este protocolo, las herramientas y las capacidades adicionales que posee. Se encuentra disponible para gestionar tanto dispositivos de red como sistemas operativos UNIX.



Figura 21. OpenSSH es la implementación de SSH más utilizada en el mundo. En el sitio web del proyecto podemos encontrar gran cantidad de información de interés (www.openssh.com).

En los siguientes comandos podemos observar cómo se utiliza el comando **scp** (incluido en el proyecto OpenSSH), para realizar la transfe-

rencia de archivos entre servidores, utilizando canales encriptados. Se puede ver claramente cómo se utilizan claves criptográficas RSA para la autenticación de los equipos.

```
fabian@debian:~$ scp 192.168.0.115:./archivo.txt ./
Authenticity of 192.168.0.115 can't be established
RSA key fingerprint is 01:18:46:a8:02:37:dc:6b:e3:dd:e2:ba:c8:0c:bb:44.
Are you sure you want to continue(yes/no)? yes
Added '192.168.0.115' to the list of known hosts.
fabian@192.168.0.115's password:
archivo.txt      100%  0  0.0KB/s  00:00
```

Además de **scp**, podemos utilizar herramientas de entorno gráfico, mucho más amigables, como **WinSCP** (<http://winscp.net>).

TLS

Transport Layer Security y su predecesor, *Secure Socket Layer* (SSL) permiten agregar una capa de seguridad a otros protocolos, utilizando una mezcla de criptografía simétrica y asimétrica para garantizar la privacidad e integridad de los datos.

TLS suele ser de mucha utilidad para proteger protocolos como HTTP y SMTP, que no fueron desarrollados para proteger los datos que intercambian.

Más allá de esto, debemos recordar que el hecho de proteger el tráfico encriptándolo no nos libera de otro tipo de ataques, como por ejemplo los ataques de fuerza bruta y los exploits, entre otros.

TLS SE ENCARGA DE
AGREGAR UNA CAPA
DE SEGURIDAD
A OTROS
PROTOCOLOS





Figura 22. Stunnel nos permite proteger aplicaciones utilizando TLS. Puede ser de mucha utilidad para dotar a nuestros programas o servicios inseguros de una buena capa de seguridad, sin requerir mayores esfuerzos (www.stunnel.org).

SMTP, IMAP y POP3

Estos tres protocolos son los más utilizados por las arquitecturas de correo electrónico. El primero, *Simple Mail Transfer Protocol*, sirve para transportar los mensajes de correo. Los dos últimos, *Internet Message Access Protocol* y *Post Office Protocol 3*, son empleados para que los usuarios accedan a los correos que están alojados en los servidores.



ANÁLISIS CONTINUO DE LA RED



Debemos analizar constantemente nuestra red en búsqueda de protocolos extraños o no permitidos, debido a que es posible conocer qué herramientas o software están utilizando los servidores y estaciones de trabajo si sabemos qué tipo de datos transmiten. Son varias las aplicaciones malintencionadas que generan ciertos patrones de tráfico detectables.

Como la mayoría de los protocolos TCP/IP, estos tres envían y reciben la información en texto plano, por lo que son muy vulnerables a las capturas de tráfico. Actualmente, muchos de los servicios más populares de correo soportan el uso de TLS para proteger a estos protocolos (que en su versión segura se llaman SMTPS, IMAPS y POP3S). Es ampliamente recomendable emplear las versiones seguras de ellos.

En el caso de SMTP, además de la encriptación de tráfico, es importante utilizar medidas de seguridad para bloquear los intentos de enviar spam a través de nuestros servidores. Esto es particularmente importante porque podríamos terminar en las listas negras y nuestros servidores serían bloqueados, lo que causaría la pérdida de varios correos.

```
fabian@debian:~$ telnet smtp.gmail.com 25
Trying 74.125.159.109...
Connected to gmail-smtp-msa.l.google.com.
Escape character is '^]'.
220 mx.google.com ESMTP
HELO fabian
250 mx.google.com at your service
MAIL FROM: fabian@portantier.com
530 5.7.0 Must issue a STARTTLS command first.
```

En el código anterior, podemos ver cómo al intentar enviar un correo, los servidores de Gmail nos obligan a utilizar TLS para autenticarnos y encriptar las comunicaciones.

HTTP y FTP

Hyper Text Transfer Protocol y también *File Transfer Protocol* son los protocolos utilizados habitualmente para transferir archivos y documentos a través de las redes. El uso más frecuente de HTTP es servir las páginas de los sitios web.

Tanto HTTP como FTP envían y reciben los datos en texto plano, lo que los hace muy inseguros si necesitamos transferir información confidencial o credenciales de acceso.

En el caso de HTTP, existen dos formas para solicitar credenciales de autenticación: **Basic** y **Digest**. En la primera, el usuario y la contraseña se envían directamente sin encriptar, por lo que es fácilmente capturable. Con respecto al método Digest, se utiliza encriptación para transmitir las credenciales. Aun así, podemos ser víctimas de un ataque del tipo *Man-in-the-middle* (que consiste en que un atacante se interponga entre el cliente y el servidor, capturando y hasta modificando el tráfico entre ambos), debido a que no se valida al cliente en sí. Además, solo se están protegiendo las credenciales enviadas, y no los datos que pueden ser transferidos después.



Figura 23. Hakipedia es un sitio web del tipo wiki en el cual podemos encontrar descripciones de varios tipos de ataque. Es un excelente recurso de información para mantenernos actualizados (www.hakipedia.com).

Evidentemente, la seguridad de estos dos protocolos es muy pobre, y es por eso que se recomienda utilizar TLS para agregar encriptación y autenticación del cliente. Las versiones de dichos protocolos se conocen

como HTTPS y FTPS. En el caso de FTP, podemos considerar la opción de reemplazarlo por SFTP, que es un método de transferencia de archivos que utiliza SSH para brindar seguridad.

DHCP

Dynamic Host Configuration Protocol permite a los clientes de una red obtener sus parámetros de configuración automáticamente. Aunque en general se utiliza solo para que los clientes obtengan la información de dirección IP, puerta de enlace y servidores DNS, el protocolo tiene muchas más opciones y parámetros.



Figura 24. La herramienta **DHCP-Probe** nos permite detectar los servidores DHCP que se encuentran en una red local. Es de mucha utilidad para detectar servidores que no deberían estar ahí (www.net.princeton.edu/software/dhcp_probe).

Como es un protocolo que fue desarrollado para ser muy simple, también es muy inseguro. Un atacante podría utilizar nuestros servidores DHCP para obtener una dirección de red válida y consultar información de la red. También es sencillo crear un servidor DHCP para confundir a los otros clientes de

la red, o generar un pequeño programa que envíe múltiples peticiones al servidor, haciendo que las direcciones disponibles para asignar se agoten.

Para evitar ataques, la mejor opción es monitorear los registros de sistema a fin de detectar comportamientos extraños. También debemos estar alertas acerca de la cantidad de direcciones sin asignar de las que disponemos. Es una excelente idea monitorear la red en busca de servidores DHCP adicionales. Otra medida de seguridad muy habitual es definir una lista de direcciones MAC a las cuales responderá nuestro servidor DHCP, y hacer que se registren como alertas las peticiones que vengan de direcciones MAC que no estén en esa lista. Cabe destacar que varios de estos problemas de seguridad son solucionados con el uso de IPv6.

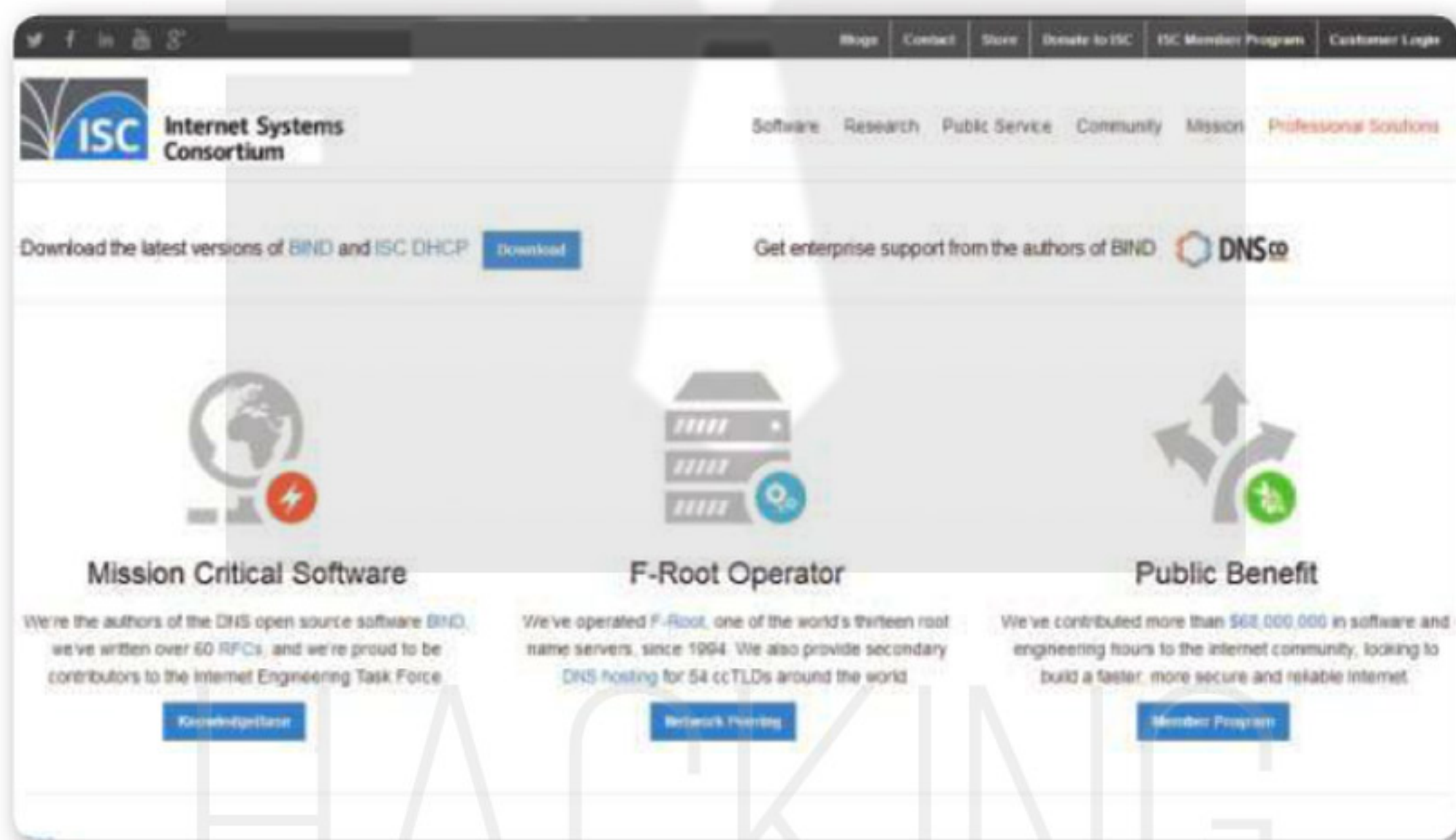


Figura 25. El **Internet Systems Consortium (ISC)** desarrolla, entre otros, el famoso servidor de DNS de código abierto BIND.

También mantiene software de cliente y servidor DHCP (www.isc.org).

DNS

Domain Name System se utiliza, entre otras cosas, para que las computadoras puedan resolver nombres de dominio a direcciones IP.

También es usado para determinar cuáles son los servidores SMTP que corresponden a un determinado dominio.

Los servidores DNS representan una pieza crítica de la infraestructura de las redes e internet. Si un atacante consigue tomar el control de nuestros servidores DNS, tiene la posibilidad de realizar varios subataques con grandes posibilidades de éxito, como, por ejemplo, el *phishing*.

LOS SERVIDORES
DNS SON UNA PIEZA
CRÍTICA DE LA
INFRAESTRUCTURA
DE INTERNET

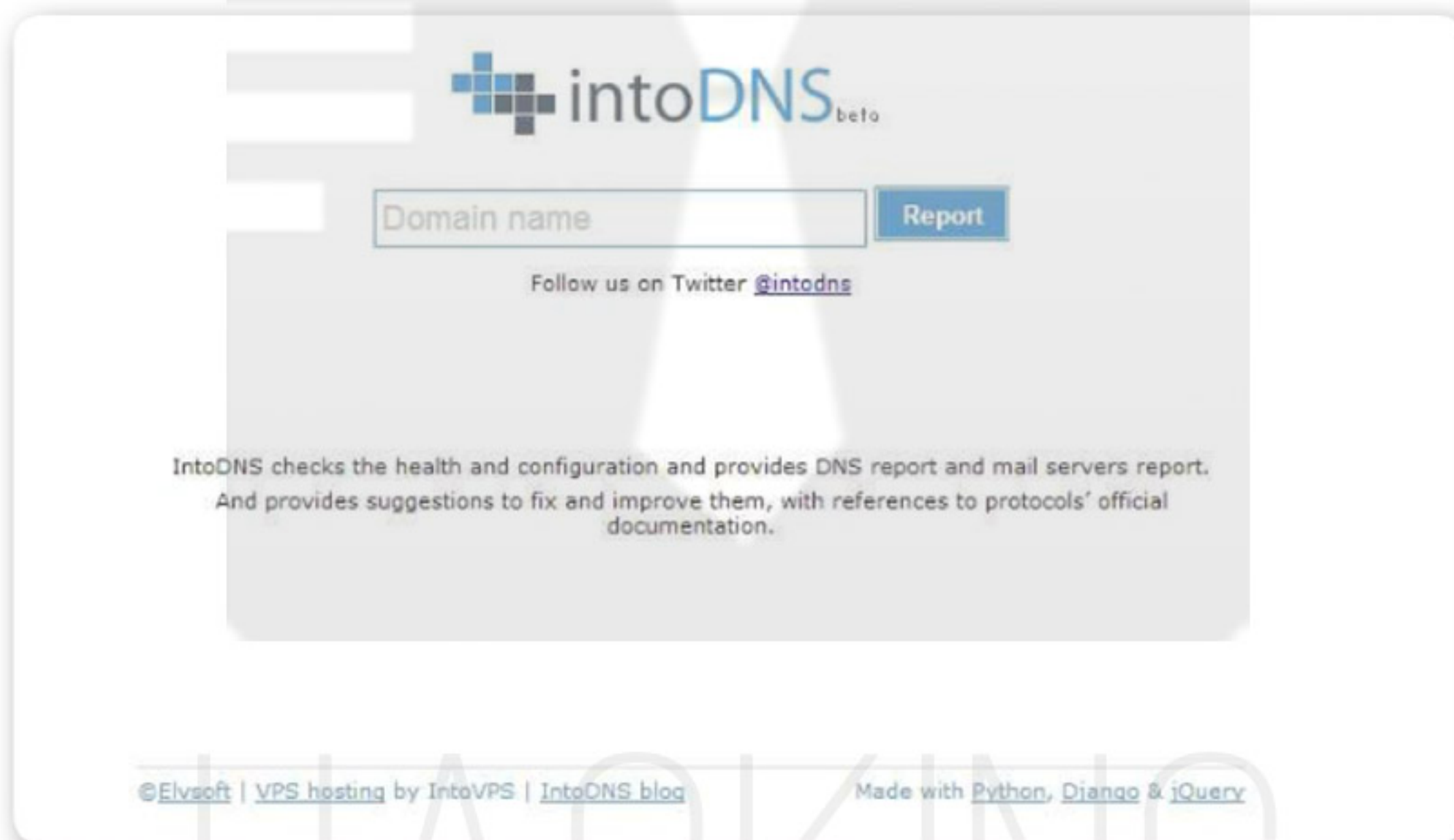


Figura 26. Existen varios sitios web que nos permiten comprobar errores en la configuración de los DNS de un dominio de forma rápida y gratuita. Algunos son: **www.intodns.com**, **www.dnscolos.com**, **www.dnssy.com** y **www.dnscog.com**.

Particularmente, el diseño del protocolo DNS no presenta mayores inconvenientes de seguridad, pero debemos prestar especial atención a este tipo de servidores con respecto a una mala configuración, que podría exponer información confidencial de nuestra organización y los dominios de los cuales somos responsables.



Figura 27. La organización IETF ha desarrollado un conjunto de extensiones para securizar los servicios DNS, permitiendo que sea validada la autenticidad de quien origina la respuesta a una consulta, además de garantizar la integridad de los datos (www.dnssec.net).

SNMP

Simple Network Management Protocol se utiliza, habitualmente, para consultar o modificar información en los dispositivos de telecomunicaciones, como routers, switches y firewalls, aunque también existen versiones disponibles para UNIX y Windows. Ofrece una manera fácil de acceder a la información del equipo y a cada una de sus interfaces. La mayoría de las herramientas de monitoreo lo utilizan en mayor o menor medida.

```
snmp-server view ReadView system included
snmp-server group ReadOnly v3 auth read ReadView
snmp-server user fabian ReadOnly v3 auth md5 mipassword priv des56 pfpfpf
```


Con el comando de arriba hacemos lo siguiente:

Creamos la vista denominada **ReadView**, que solamente puede leer los atributos dentro de **system**.

Creamos el grupo **ReadOnly**, de SNMPv3, con la vista ReadView.

Creamos el usuario **fabian**, del grupo **ReadOnly**, de SNMPv3, con la contraseña **mipassword**, encriptada con MD5 y el tráfico encriptado con DES56, utilizando la clave **pfpfpf**.

Para verificar nuestra configuración, podemos utilizar los comandos que mostramos a continuación:

```
show snmp view  
show snmp group  
show snmp user
```

Como el requerimiento principal fue la simplicidad, con el correr de los años fue necesario hacer modificaciones que respondieran a los requerimientos de seguridad actuales.

Las versiones más populares disponibles en varios dispositivos y sistemas operativos son la 1, 2c y 3.

Las versiones **1** y **2c** utilizan como único método de seguridad el concepto de comunidades, que son algo así como contraseñas, que definen si se tienen permisos de lectura o lectura/escritura. Como el tráfico viaja en texto plano a través de la red, existen grandes posibilidades de que nuestras credenciales sean vistas por alguien que esté capturando paquetes en ella.

La **versión 3** del protocolo agrega varias capacidades de seguridad, entre ellas, encriptar el tráfico, utilizar credenciales del tipo usuario/contraseña y permitir la definición de distintas vistas por usuario. Es evidente que solo esta versión cumple con los requisitos de seguridad actuales, de modo que debemos tenerlo en cuenta al seleccionar los equipos de telecomunicaciones que vamos a adquirir.



Diseño de redes seguras

Con respecto a la seguridad de las redes, no todo es gestión y configuración. También existe un aspecto de suma importancia, que es el diseño. Para cuestiones tanto de seguridad como de rendimiento, el diseño, la selección de equipamiento y la disposición de los equipos, determinarán las capacidades con las que contará la red. Por eso es tan importante prestar atención al diseño, sobre todo, si tenemos la capacidad de construir la red desde cero y, en caso de que estemos trabajando con una red ya construida, analizar cómo podemos mejorarla constantemente.

Llevando el ejemplo al extremo, la red más insegura es aquella que se denomina **plana**, en la cual todos los equipos tienen conectividad abierta entre unos y otros, sin ningún tipo de filtrado. En este caso, la seguridad quedaría relegada únicamente a las estaciones de trabajo y los servidores, que deberían protegerse cada uno por su cuenta. Como vimos en el **Capítulo 1**, el concepto de **defensa en profundidad** nos lleva a implementar varios controles en todos los puntos que sea posible. Así que debemos prestar mucha atención a las opciones de seguridad que ponen a nuestra disposición los dispositivos de telecomunicaciones.

También debemos tener en cuenta que una conexión que no puede realizarse no puede ser utilizada para atacar a un sistema. Entonces, es mucho más sencillo filtrar conexiones que intentar protegerlas con métodos complejos.

Zonas desmilitarizadas

También conocidas como **DMZ**, sirven para ubicar dispositivos que presten servicios públicos a través de internet. Estos servicios, por naturaleza, se encuentran mucho más expuestos que los utilizados solamente para propósitos internos.

En caso de que, por ejemplo, un atacante pueda tomar el control de nuestro servidor web, esta separación complicaría el acceso desde allí hacia la red local (LAN). Por lo tanto, es necesario implementar este tipo



de separaciones siempre que contemos con servidores expuestos a redes públicas, como internet. También es recomendable utilizarlas para colocar los equipos destinados a conexiones con organizaciones asociadas, clientes o proveedores.

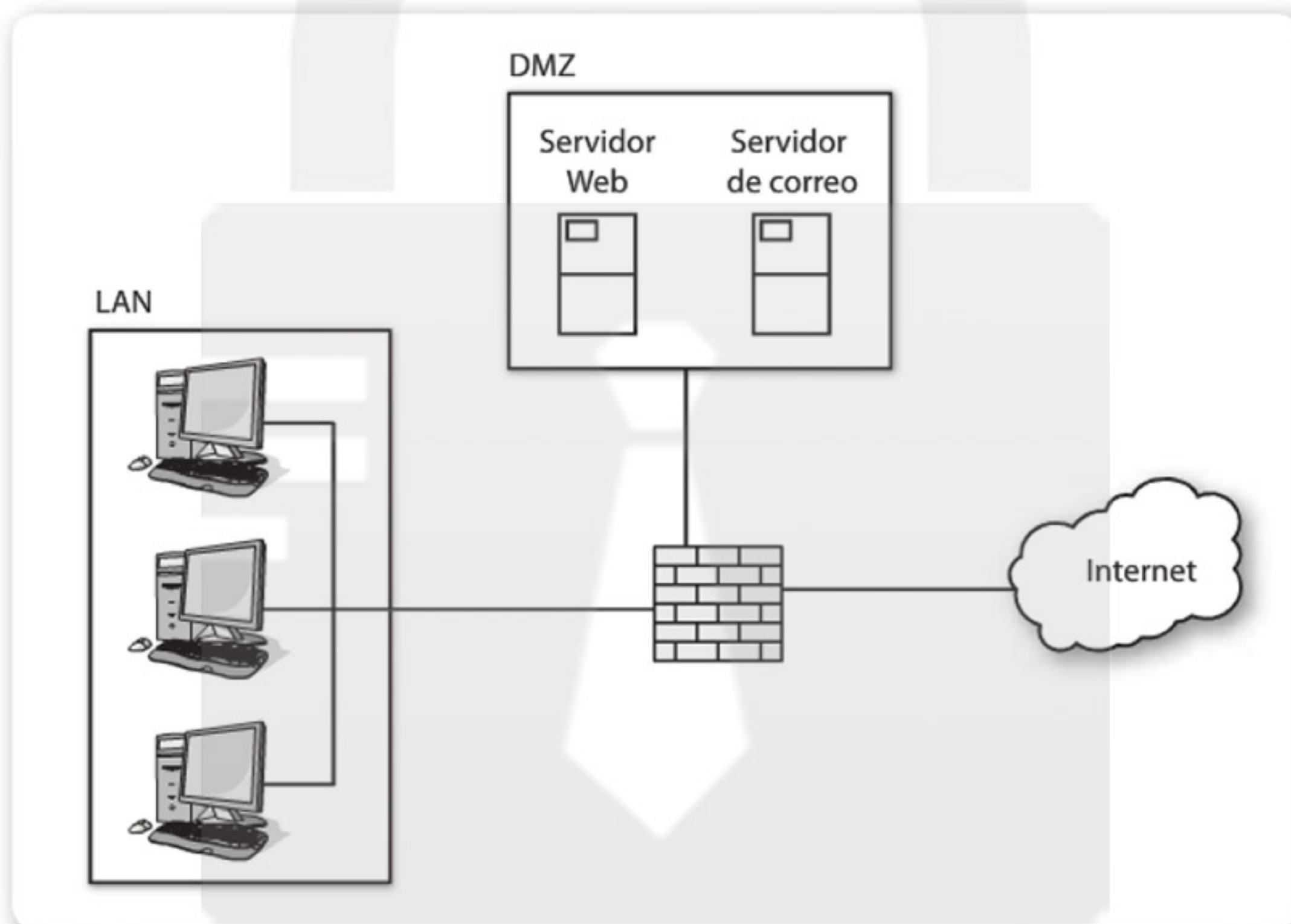


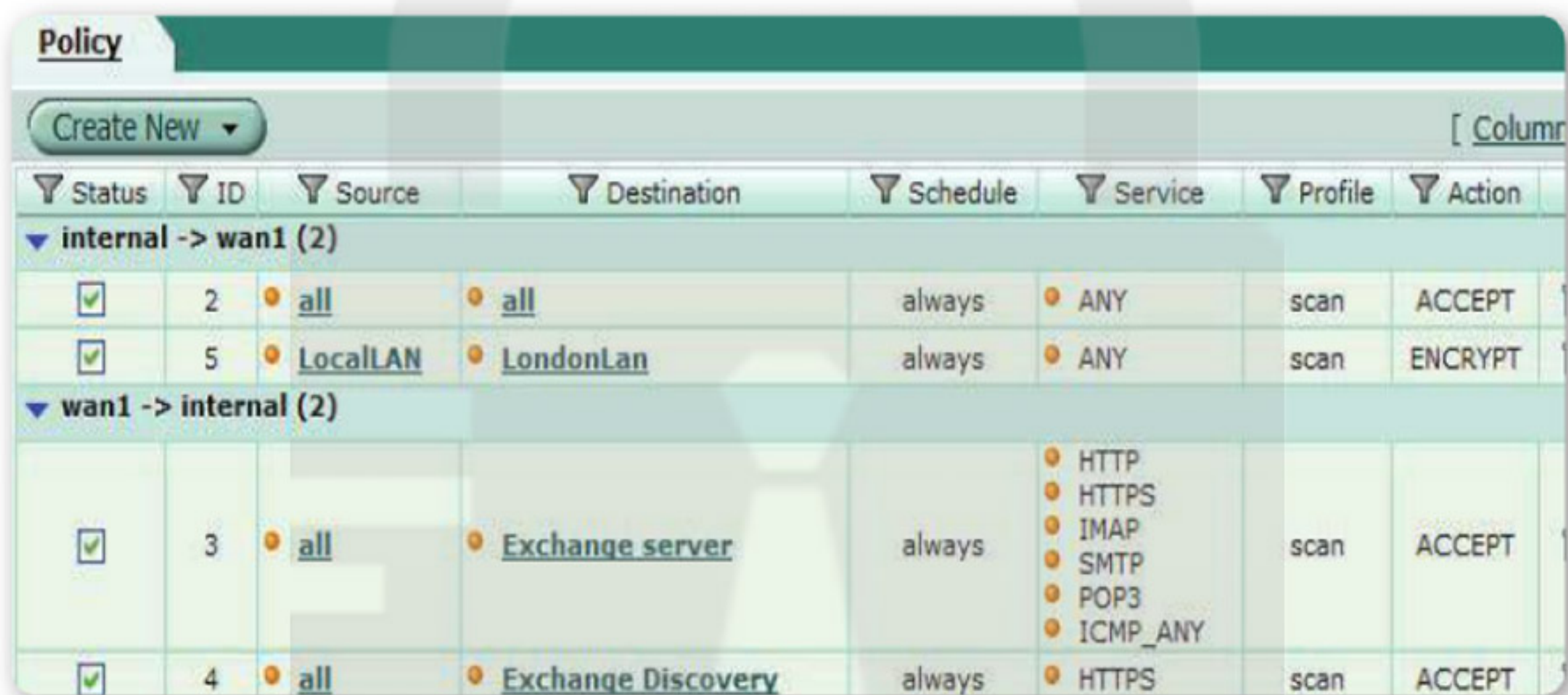
Figura 28. El diagrama muestra un diseño típico de la separación a través de un firewall de la red local, la DMZ e internet.

Estas separaciones pueden crearse utilizando firewalls, routers o un servidor dedicado a esta tarea. Entre todas estas opciones, cada una tiene sus ventajas y desventajas, de las cuales mencionamos algunas en el siguiente apartado.

Firewall

Es la opción más recomendable en todos los casos, sobre todo, porque se trata de equipos ya preparados para esta tarea y suelen contar

con opciones que nos serán de mucha utilidad. Algunos nos permitirán implementar controles antivirus y capacidades de NIDS, que van a reforzar mucho la seguridad entre la LAN y la DMZ. Además, suele ser la opción más sencilla de administrar, mantener y monitorear.



Status	ID	Source	Destination	Schedule	Service	Profile	Action
▼ internal -> wan1 (2)							
☒	2	all	all	always	ANY	scan	ACCEPT
☒	5	LocalLAN	LondonLan	always	ANY	scan	ENCRYPT
▼ wan1 -> internal (2)							
☒	3	all	Exchange server	always	HTTP HTTPS IMAP SMTP POP3 ICMP_ANY	scan	ACCEPT
☒	4	all	Exchange Discovery	always	HTTPS	scan	ACCEPT

Figura 29. En la imagen podemos ver una captura de pantalla de la interfaz de configuración web de un equipo **Fortigate**, de la empresa **Fortinet**. Como podemos observar, presentan una interfaz sencilla, pero al editar cada una de las políticas podemos configurar opciones avanzadas, como detección de **Malware** e **IDS**.

Router

En caso de que no contemos con un firewall, podemos optar por utilizar un router y configurar una buena cantidad de listas de control de acceso, para tener bien limitado el tipo de conexiones que pueden realizarse de un lugar a otro. Con estos filtros bien configurados, podemos tener un buen nivel de seguridad, sin entrar en los costos que puede representar un firewall.

A continuación podemos ver un ejemplo de listas de control de acceso (ACL) en un router Cisco, el cual solamente permite tráfico DNS, HTTP, SMTP y también POP3.


```
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit udp any any eq domain
access-list 102 permit udp any eq domain any
access-list 102 permit tcp any any eq domain
access-list 102 permit tcp any eq domain any
```

Servidor

Esta es una opción que puede resultar interesante, sobre todo para los profesionales que cuenten con experiencia en sistemas operativos de código abierto, como GNU/Linux y BSD. Podemos instalar alguna de las distribuciones que están desarrolladas específicamente para ser utilizadas como firewalls. Puede ser la opción más económica, pero debemos tener en cuenta los problemas de disponibilidad que podemos llegar a tener en caso de que el servidor presente una falla de hardware.

Al seleccionar la opción que vamos a utilizar, es preciso tener en cuenta tanto nuestras capacidades económicas, como nuestras necesidades y conocimientos técnicos para concretar la solución. Como la mayoría de las conexiones permitidas serán desde la LAN hacia la DMZ por propósitos de gestión de los equipos, no es necesaria capacidades avanzadas de filtrado.



SEPARACIONES DE RED



Debemos prestar atención a las separaciones de red tanto físicas como lógicas, manteniendo dos diagramas de topología distintos. Debido a que cada una de ellas representa diferentes medidas de seguridad, siempre hay que tener en cuenta que una separación lógica puede fallar por cuestiones de configuración, pero una física no.

Separación de VLANs

Virtual Local Area Network es un método para crear redes lógicamente independientes dentro de una misma red física. Para realizar esto, los paquetes son marcados con un campo especial, denominado etiqueta o tag, que identifica a las distintas VLANs. Dicho tag se ubica como un campo adicional en la estructura de datos de cada paquete transmitido.

Esto nos permite tener el tráfico separado por medio de los switches y filtrar la conectividad entre los dispositivos, aunque se encuentren compartiendo un mismo medio físico. El estándar que actualmente se utiliza en la mayoría de las implementaciones de VLANs es el IEEE 802.1Q

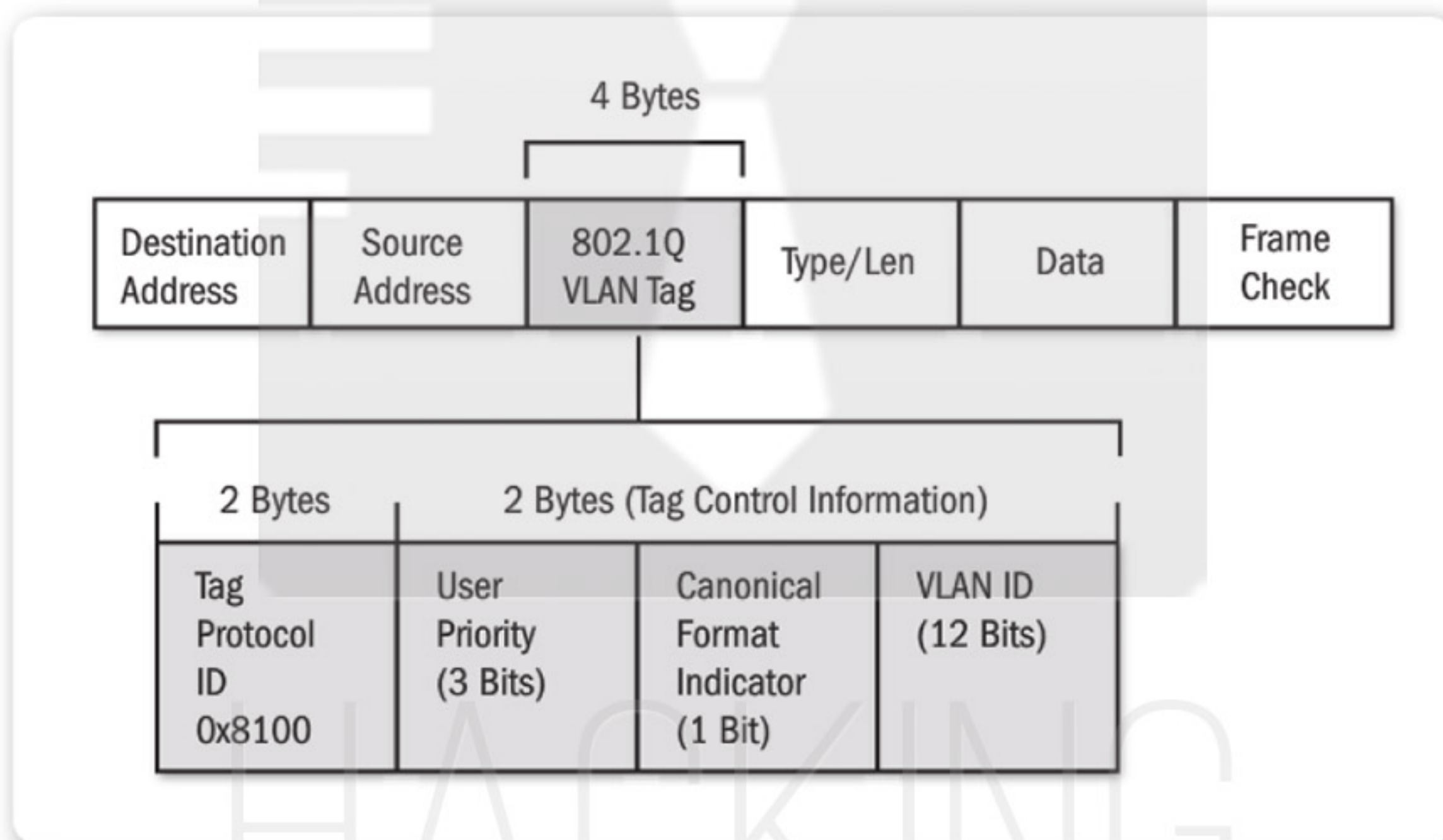


Figura 30. El diagrama muestra cómo se agregan 4 bytes a la trama Ethernet para los campos del protocolo **802.1Q**.

Entre algunas de las ventajas que nos brinda tener nuestro tráfico separado por VLANs, podemos enumerar los siguientes:

- Delimitar los dominios de broadcast, para mejorar el rendimiento.
- Organizar mejor la red y los dispositivos que están conectados a ella.



- Disminuir la posibilidad de accesos no autorizados y escuchas de tráfico.

Como podemos notar, es de utilidad implementar separación de VLANs no solamente para propósitos de seguridad, sino también para mejorar el rendimiento de nuestra red. Esta es una capacidad con la que cuentan todos los switches actuales, tanto de fabricantes reconocidos, como de segundas marcas.

Es ampliamente recomendable clasificar los tipos de tráfico que tendremos en nuestra red y, sobre esa base, definir distintas VLANs. En general, la clasificación adecuada estará basada en sectores de la organización, y podrá ser, por ejemplo: **Finanzas, Marketing, Atención al cliente, Servidores**, etcétera.

También debemos tener en cuenta que ciertas tecnologías tienen requerimientos específicos en cuanto al rendimiento de la red; sobre todo, las tecnologías para transmisión de audio y video. Es por esto que se recomienda utilizar una VLAN dedicada para este tipo de tráfico.

También es de suma importancia reservar una VLAN exclusivamente para la administración de dispositivos, es decir, protocolos SNMP, SSH, etc. Esto nos permitirá conservar la gestión de los equipos, aun cuando la red esté saturada. Mantener este tipo de tráfico dividido del resto también nos servirá para implementar filtros más granulares acerca de qué estaciones de trabajo pueden administrar remotamente los dispositivos de red.

En el siguiente ejemplo, veremos una configuración de VLANs de un equipo Cisco Catalyst 2924 XL, en la que separamos el tráfico de voz sobre IP (VoIP) de los tráficos de estaciones de trabajo y servidores.

```
vlan database
(vlan)#vtp transparent
Setting device to VTP TRANSPARENT mode.
(vlan)#vlan 10 name Workstations
VLAN 10 added:
```



```
Name: Workstations
(vlan)#vlan 20 name Servers
VLAN 20 added:
  Name: Servers
(vlan)#vlan 30 name VoIP
VLAN 30 added:
  Name: VoIP
(vlan)#exit
APPLY completed.
Exiting....
```

Redes privadas virtuales

Las conexiones VPN (*Virtual Private Networks*) deben ser utilizadas siempre que necesitemos realizar conexiones seguras sobre medios no seguros (como internet). Este tipo de herramienta es de suma utilidad para habilitar el trabajo remoto y permitir que los empleados de la organización se conecten a nuestra red desde sus hogares u otros sitios. También es útil para conectar varias sucursales a una casa central.

MUCHOS
DISPOSITIVOS UTM
PUEDEN
FUNCIONAR COMO
CONCENTRADORES VPN



Muchos de los dispositivos UTM pueden funcionar como concentradores de VPN, y los sistemas operativos UNIX cuentan con herramientas para el mismo propósito, generalmente, utilizando protocolos como IPSec y SSL/TLS, con algoritmos de encriptación como AES y 3DES y funciones de hash como MD5 y SHA. Cualquiera sea la combinación de estas herramientas, nuestras conexiones permanecerán relativamente seguras, con la única vulnerabilidad de que las credenciales

de acceso puedan ser adivinadas o conseguidas por medios que no tengan que ver con la conexión VPN en sí.

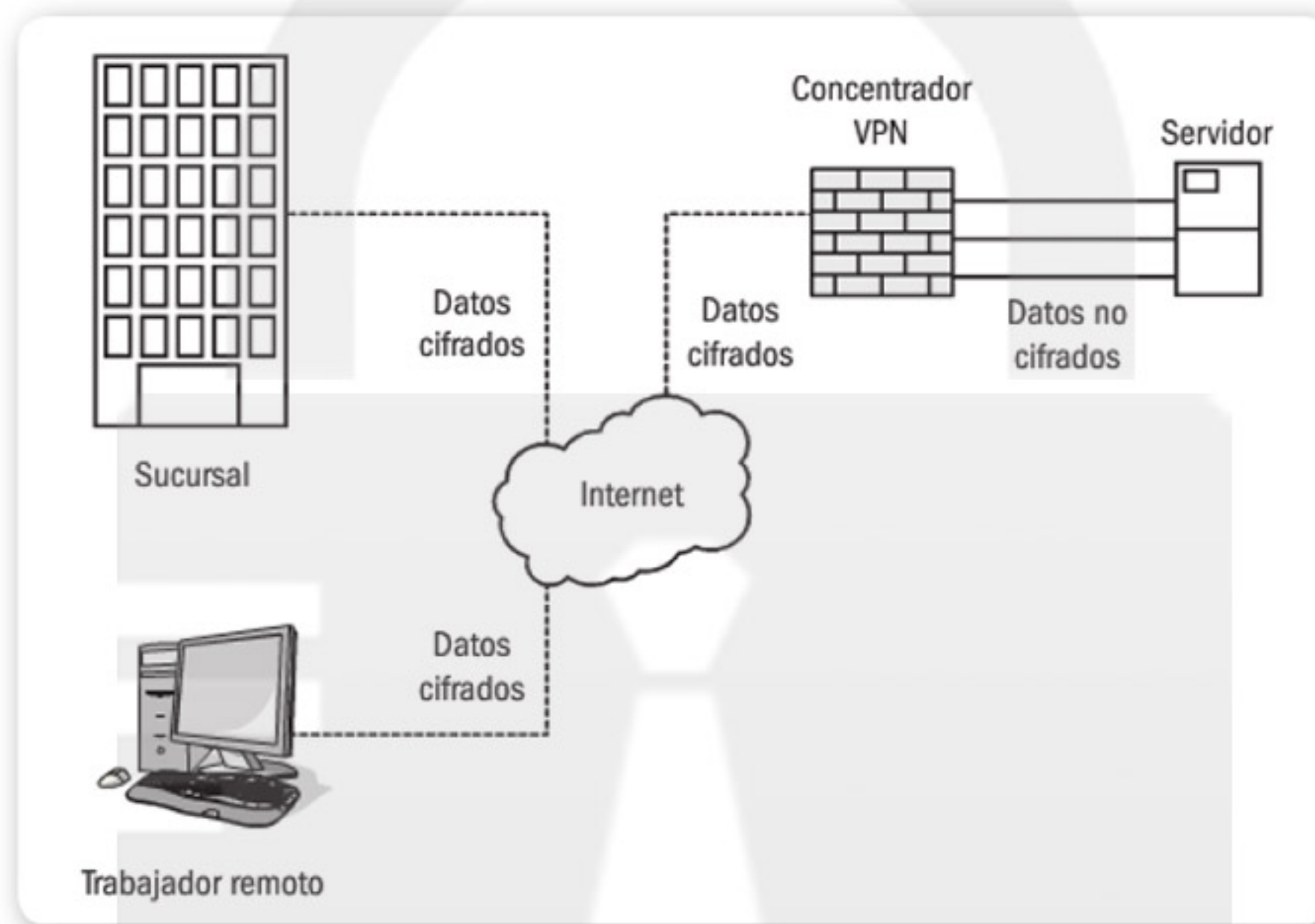


Figura 31. El diagrama muestra cómo es posible utilizar una **VPN** para proteger el tráfico tanto de conexiones de usuarios remotos como de sucursales en una casa central, a través de un concentrador de conexiones VPN.



RESUMEN

En este capítulo reafirmamos la importancia de contar con un sólido inventario de los dispositivos que se encuentran en la red, vimos algunas herramientas que nos ayudan en esta tarea y analizamos los dispositivos más utilizados en la mayoría de las empresas: routers y switches. Más adelante vimos las configuraciones de seguridad más comunes ofrecidas por estos dispositivos de red. Conocimos los detalles relacionados con el funcionamiento de los firewalls y aprendimos las vulnerabilidades que pueden presentarse con el uso de una red inalámbrica. Analizamos la forma de realizar una efectiva protección contra intrusos y aprendimos a administrar en forma remota.

Actividades

TEST DE AUTOEVALUACIÓN

- 1 ¿Por qué debemos prestar atención a la seguridad de routers y switches?
- 2 ¿Qué diferencia existe entre los sistemas IDS e IPS?
- 3 Explique qué es SSH.
- 4 ¿De qué forma podemos proteger el tráfico de los protocolos que envían los datos en texto plano?
- 5 ¿Con qué dispositivos podemos dividir la red LAN de la DMZ?



PROFESOR EN LÍNEA



Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: **profesor@redusers.com**

Sistemas operativos

En este capítulo veremos la forma correcta de seleccionar y asegurar sistemas operativos, detallaremos los protocolos de gestión adecuados y también revisaremos los detalles relacionados con los distintos tipos de autenticación.

▼ Características	140	▼ Servidores de autenticación ...	165
▼ Windows vs. UNIX.....	141	▼ Análisis de logs.....	167
▼ Hardening	144	▼ Administración remota	170
▼ Network Access Control	150	▼ Detección de intrusos	177
▼ Malware	152	▼ Gestión de parches.....	180
▼ Firewalls	155	▼ Resumen	181
▼ Backups	157	▼ Actividades	182
▼ Autenticación multifactor	161		



Características

Los **sistemas operativos** representan un alto valor, tanto para las organizaciones como para sus posibles atacantes. Esto se debe, principalmente, a que son los encargados de almacenar y procesar la información, lo que hace que una falla en ellos puede ser causa de pérdida de datos, robo de datos y otros problemas serios.

Como todas las tecnologías, estos sistemas han evolucionado constantemente, y se volvieron más seguros con el correr de los años. Pero también tuvieron que adaptarse a las nuevas necesidades del mercado, aumentando las capacidades de conectividad y la diversidad de las funcionalidades prestadas, lo cual abre las puertas a nuevos tipos de ataques y vulnerabilidades. Es por eso que podemos afirmar que, si bien los sistemas operativos son cada vez más seguros en su diseño, presentan cada vez mayores vectores de ataque, por estar obligados a ofrecer cada vez más funcionalidades. Recordemos que, a mayor funcionalidad de un sistema, mayores son sus posibilidades de falla.

Por otra parte, podemos observar que el mercado se vuelve más exigente en cuanto a los niveles de seguridad esperados, por lo que vemos que se implementan varias tecnologías desarrolladas exclusivamente para proteger los sistemas. Este tipo de enfoque nos permite tener un mayor control de la seguridad, pero también nos obliga a estar al tanto de todas las capacidades con las que cuentan nuestros sistemas, para poder implementarlas correctamente.

En la actualidad, existen varios tipos de sistemas operativos, para diferentes propósitos, aunque podemos afirmar que la mayoría de las instalaciones en empresas pertenecen a dos grupos: **Windows** y **UNIX**. En el primer caso, podemos encontrar sistemas tanto para escritorio como para servidor. En el segundo grupo, hay una infinidad de variantes –como **GNU/Linux**, **BSD**, **HP-UX**, **IBM-AIX**, **Solaris**, etcétera–, que suelen utilizarse, principalmente, para servidores.

Si bien cada sistema operativo tiene sus particularidades que lo vuelven único, los integrantes de cada uno de estos grupos mantienen grandes



similitudes, por lo que hablaremos de sistemas Windows y sistemas UNIX, sin entrar en detalles minuciosos.

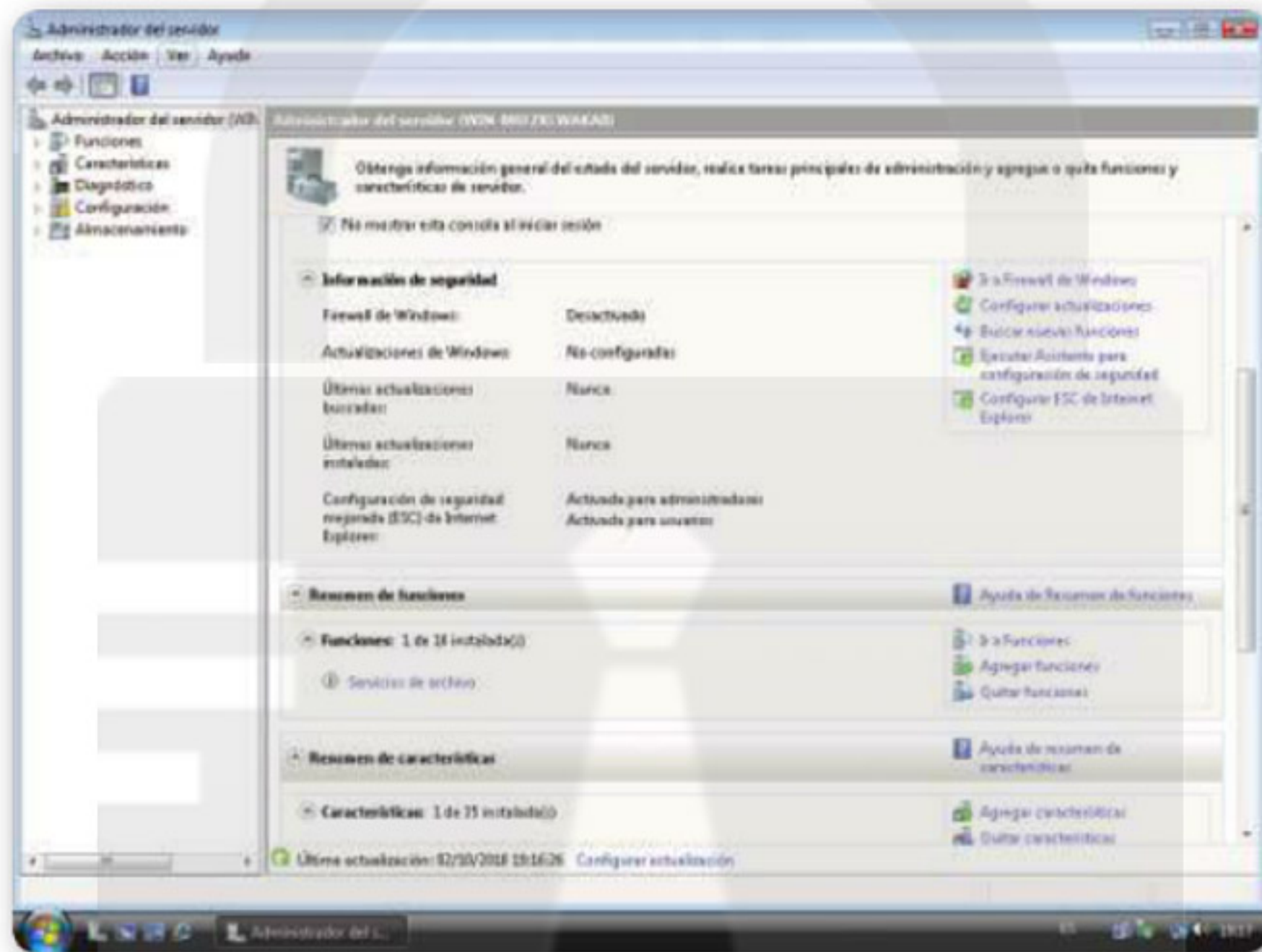


Figura 1. Windows Server 2008 es una de las versiones de este sistema más utilizadas, pues ofreció grandes mejoras de seguridad con respecto a sus versiones anteriores.



Windows vs. UNIX

En este pequeño apartado intentaremos definir un tema que se viene discutiendo hace años, y hasta llegó a definirse como la “guerra santa” del mundo informático. Nos referimos a la rivalidad entre los sistemas operativos de **Microsoft**, que son ampliamente los más utilizados del mundo, y los UNIX, que se dice que son los más seguros.

Como profesionales, debemos dejar de lado cualquier preferencia que tengamos y ser objetivos a la hora de seleccionar el mejor sistema operativo para nuestros equipos. Las falencias de los sistemas Windows han

sido muchas y muy graves, aunque, principalmente, esto estaba relacionado con el escaso interés de Microsoft por el tema seguridad.

Actualmente, esta postura ha cambiado, y podemos observar que las nuevas versiones de los sistemas operativos Windows hacen mucho más hincapié en este aspecto.

Muchos apoyan el diseño de los sistemas operativos UNIX, porque sostienen que están desarrollados desde un punto de vista más organizado y simplista. Pero, como ya mencionamos, esta es una cuestión personal y, sobre todo, depende de las necesidades del momento. Objetivamente, cada tipo de sistema operativo tiene sus ventajas y desventajas, con lo cual la elección de uno u otro estará estrictamente relacionada con el propósito del sistema. Existe una infinidad de comparativas entre estos dos tipos de sistemas, así que no vamos a reinventar la rueda en este libro.

Consejos para sistemas Windows

Este tipo de sistemas suele ser fácil de utilizar, pero no debemos dejar que esto nos lleve a subestimarlos. En sus últimas versiones, podemos apreciar que existe una gran cantidad de herramientas destinadas a aumentar la seguridad, muchas incluidas en la instalación por defecto y otras que pueden descargarse desde el sitio web del fabricante.



CUOTA DE MERCADO



Tanto los sistemas operativos Windows como los UNIX cuentan con una gran cuota de mercado y son respetables, por tener varios años de desarrollo y una gran cantidad de software disponible. Es por eso habitual el hecho de encontrar una mezcla de ambos en todas las infraestructuras tecnológicas actuales. Como buenos profesionales, debemos tener un amplio conocimiento de ambos sistemas.

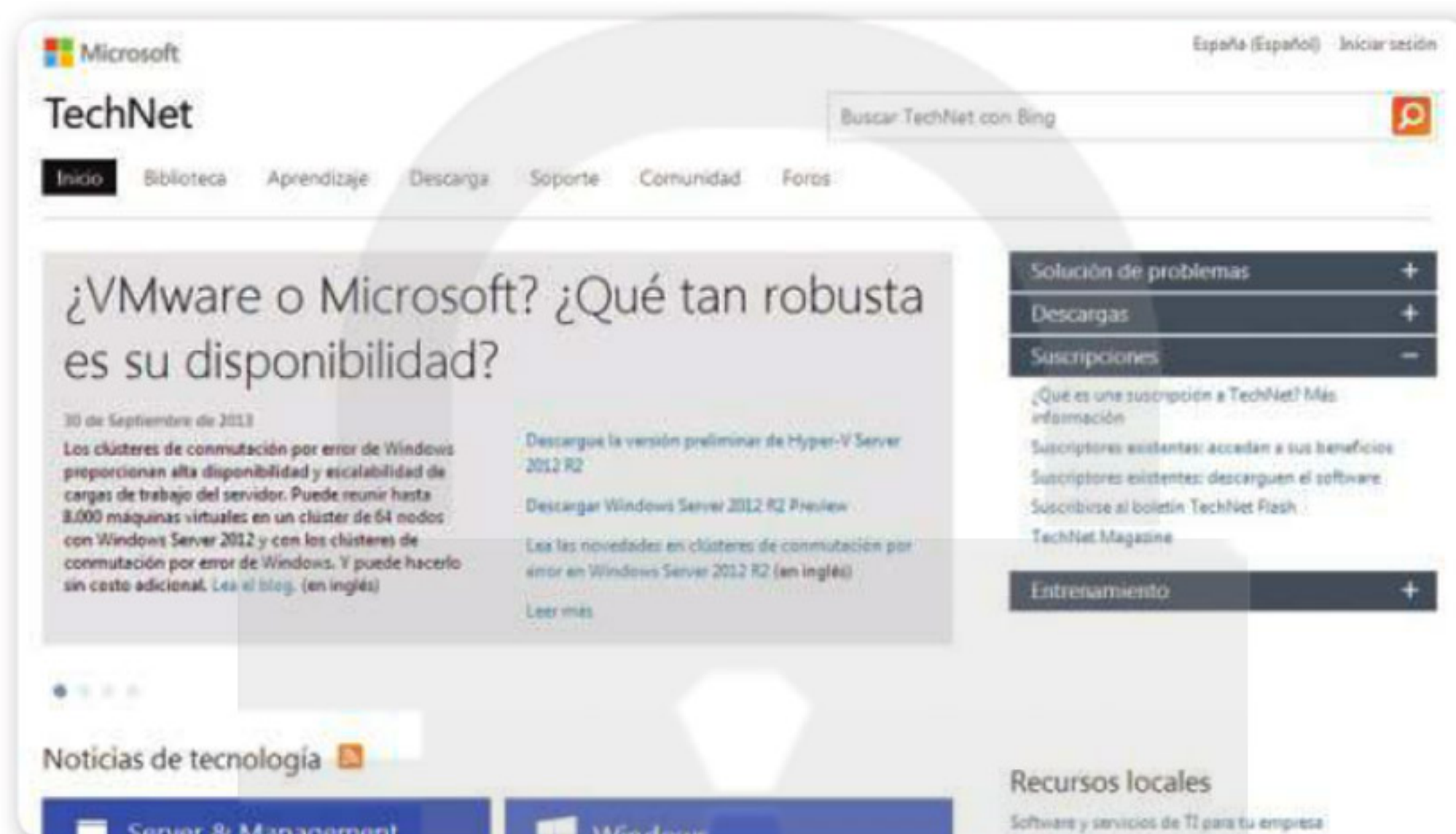


Figura 2. En <http://technet.microsoft.com> podemos encontrar innumerables recursos para aumentar la seguridad de sistemas Microsoft.

Siempre debemos prestar mucha atención a las nuevas notificaciones de seguridad y a los parches disponibles. Microsoft mantiene varios canales de comunicación para notificar a los usuarios y administradores acerca de las novedades en seguridad: desde la información básica para estar al tanto de las cosas, hasta temas más avanzados, dirigidos a administradores y pensados para darnos tiempo a preparar las acciones de aplicación de parches.

Consejos para sistemas UNIX

Estos sistemas cuentan con una gran reputación en lo que a seguridad se refiere. Pero debemos tener en cuenta que la gran cantidad de distribuciones UNIX que existen hace que cada una se enfoque en distintos objetivos, por lo que no todas pueden poner tanto énfasis en la seguridad. Es por eso que, al seleccionar el sistema UNIX que vamos a utilizar, debemos tener muchas consideraciones en mente, como las prioridades del proyecto, el soporte del fabricante, la compatibilidad de hardware, el software disponible, etcétera.

Entre las versiones libres, podemos distinguir la seguridad de los sistemas BSD (FreeBSD, NetBSD y OpenBSD), así como también de las distribuciones GNU/Linux Debian y RedHat.

Ya que estos sistemas nos permiten ser minimalistas e instalar solo lo necesario para que cumplan sus funciones, debemos planear adecuadamente qué componentes instalar y cómo configurarlos. Además, todas las versiones serias cuentan con una guía de seguridad donde se recomienda cómo realizar la configuración.



Figura 3. En www.linuxsecurity.com podemos encontrar varios recursos acerca de la seguridad en sistemas operativos GNU/Linux.



Hardening

El proceso conocido como *hardening* involucra varias tareas que buscan aumentar la seguridad de un sistema. Siempre debemos realizar dicho proceso al instalar un nuevo sistema o dispositivo. Cada sistema cuenta con sus mejores prácticas y guías que detallan cómo realizarlo adecuadamente y aprovechando todas las características de seguridad disponibles.



Sin entrar en detalles acerca de cada uno, podemos decir que el hardening se basa en las siguientes tareas:

Minimizar la cantidad de servicios utilizados: la mayoría de los sistemas operativos se instalan por defecto con una cantidad de servicios habilitados que no siempre vamos a necesitar. Por ejemplo, el enrutamiento de paquetes, las conexiones inalámbricas (incluyendo infrarrojos y Bluetooth), los puertos USB, y cualquier otro servicio que no vayamos a usar.

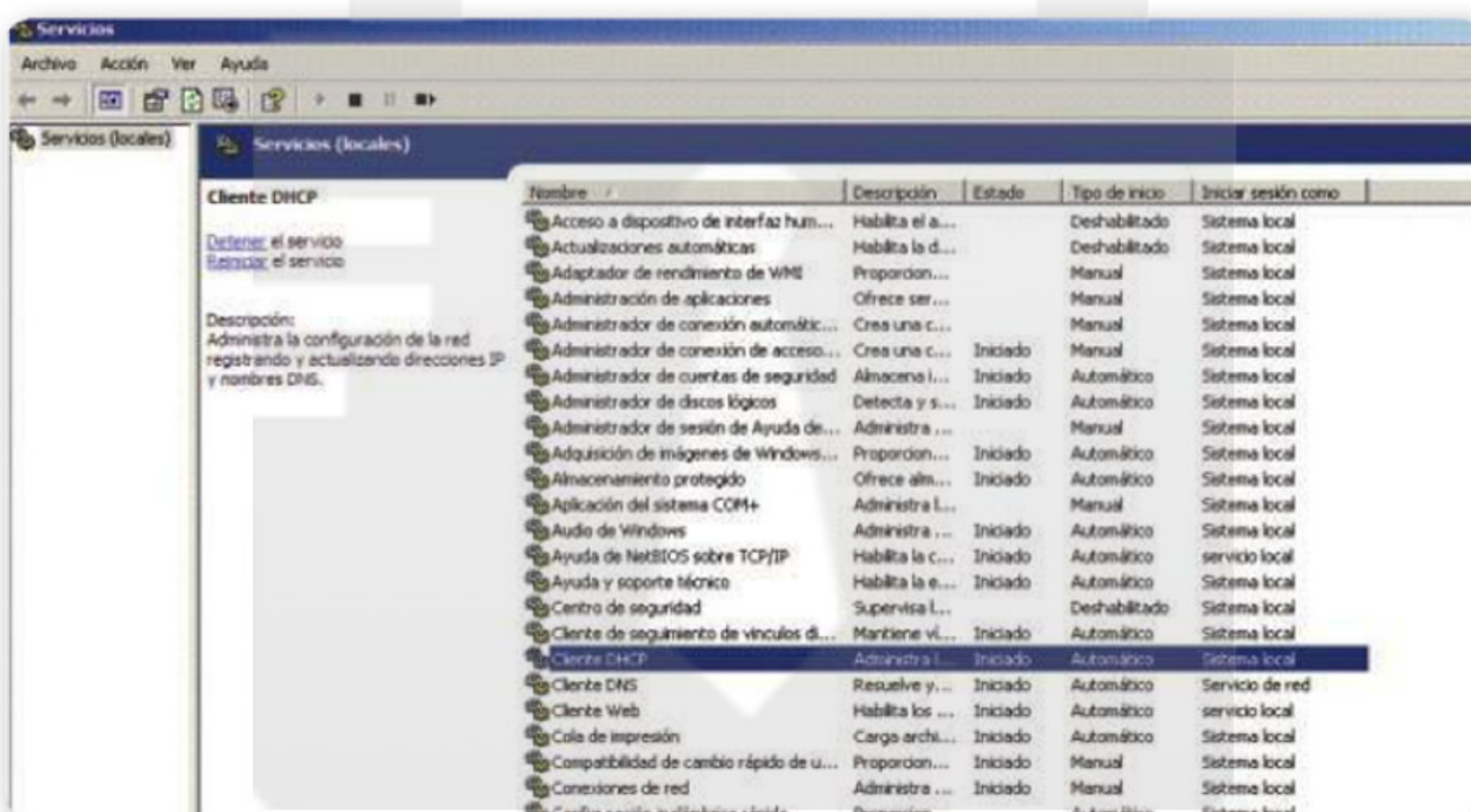


Figura 4. En la consola de administración de servicios de Windows, podemos configurar varios parámetros para cada uno de los servicios.



AUSCERT

En el caso de los sistemas UNIX, podemos basar nuestro proceso de hardening en la lista de recomendaciones publicada por el **AusCERT**, que puede consultarse en www.auscert.org.au/5816. Allí se consideran varios aspectos, tanto de los sistemas operativos UNIX en general, como de métodos para implementar las medidas en sistemas específicos.

Obviamente, dependiendo de las funciones que va a cumplir cada sistema, tendremos que seleccionar qué servicios habilitar y cuáles no. Pero debemos habilitar siempre lo mínimo necesario.

Utilizar interfaces de gestión seguras: si vamos a habilitar las interfaces de gestión remota, solamente debemos utilizar las que funcionen de forma segura, encriptando el tráfico y utilizando una buena política de accesos. Hay que considerar que, de ser posible, es recomendable realizar el filtrado de los dispositivos que podrán usarse para efectuar la administración de los sistemas en forma remota.

ES IMPORTANTE
MANTENER
EL SISTEMA
ACTUALIZADO EN
FORMA PERIÓDICA



Mantener el sistema actualizado: todos los sistemas tienen errores, que suelen ser corregidos con el lanzamiento de parches y actualizaciones. Debemos implementarlos siempre que sea posible, no solo para solucionar fallas, sino también para aprovechar funcionalidades de seguridad que pueden habilitarse con las nuevas versiones de los sistemas.

Utilizar una buena política de contraseñas: es de suma importancia que las contraseñas de acceso (tanto de usuarios como de administradores) estén obligadas a cumplir con una política que garantice la dificultad de realizar ataques de cracking sobre ellas.

Se recomienda, por lo menos, tener en cuenta los siguientes puntos:

- Tener una longitud mínima (al menos 8 caracteres).
- Realizar el cambio regular obligatorio (por ejemplo, cada 30 días).
- No repetir claves (por ejemplo, ninguna de las últimas 12).
- No utilizar palabras del diccionario.
- Emplear mayúsculas, minúsculas y números.

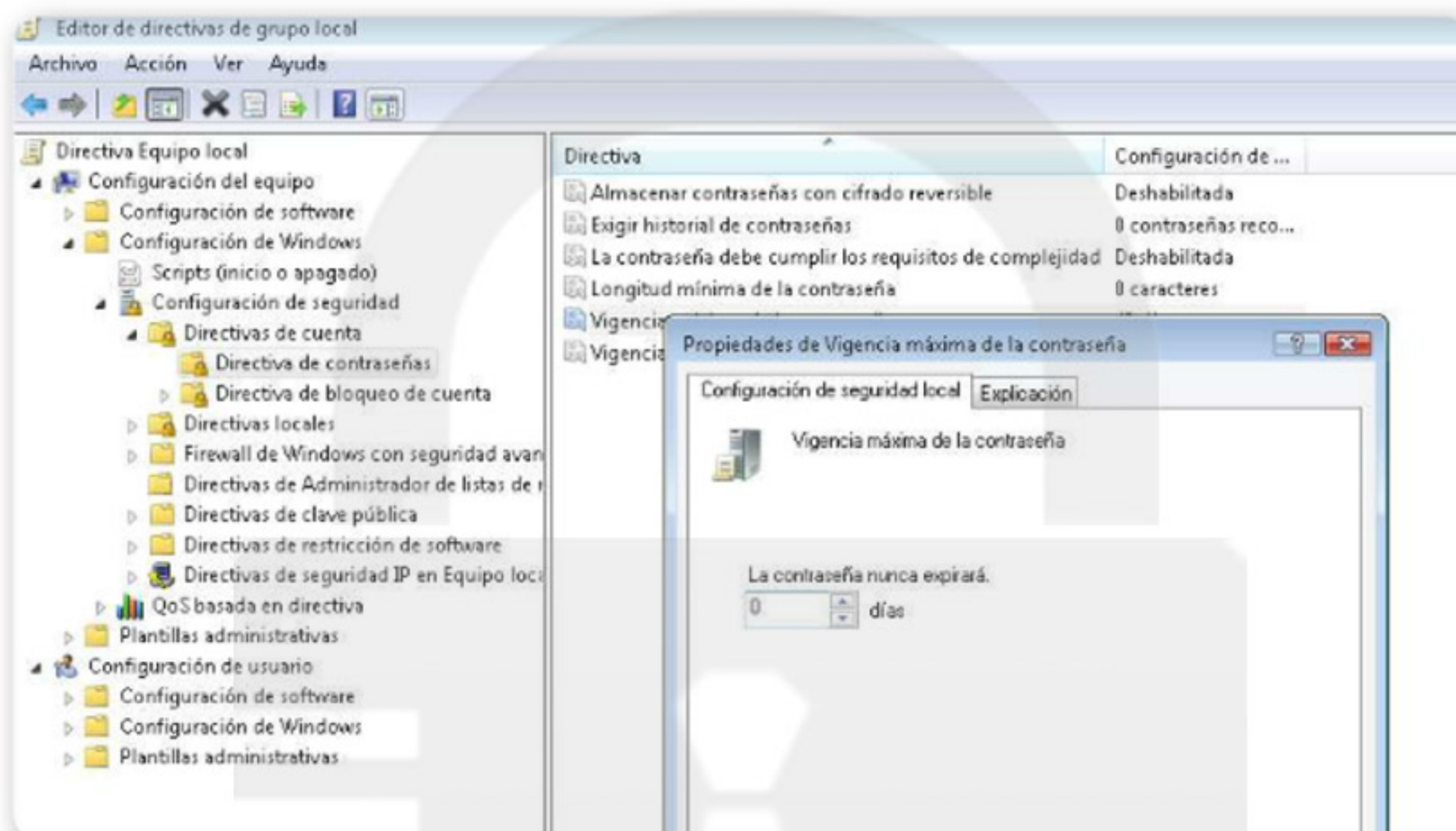


Figura 5. Los **sistemas Windows** cuentan con varias opciones de configuración para políticas de contraseñas.

Utilizar filtrado de conexiones (firewall): es recomendable implementar este tipo de filtros, por lo menos, en los servidores. Esto nos ayudará a limitar desde dónde y hacia dónde pueden establecerse las conexiones, lo cual nos permitirá evitar varios tipos de ataques a la red.



Figura 6. El firewall de Windows muestra que ha ido evolucionando con respecto a las versiones presentes en los sistemas anteriores.

Separar las particiones de disco: cuando instalamos un servidor, debemos definir un esquema de particionamiento acorde a sus tareas específicas. Por lo menos, tenemos que establecer una partición para el sistema operativo y otra para los datos que se van a almacenar en él. Esto nos permitirá reinstalar el sistema rápidamente, sin perder la información de nuestra organización.

Utilizar autenticación centralizada: los servidores de autenticación centralizada (como **ActiveDirectory**, **OpenLDAP**, y otros) nos permitirán centralizar nuestra base de datos de usuarios e implementar políticas de contraseñas de una forma sencilla.

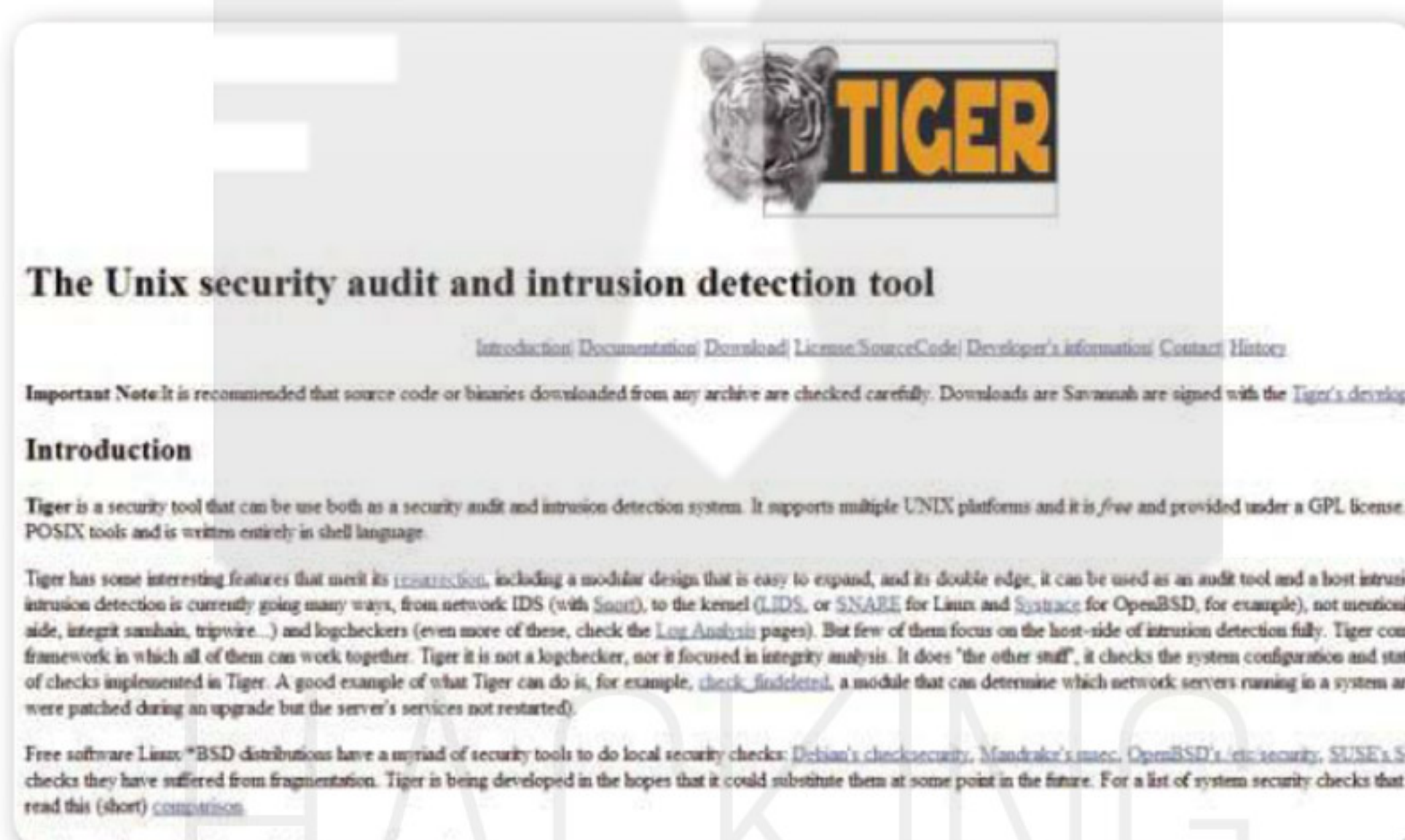


Figura 7. Tiger es un software para realizar varias comprobaciones de seguridad en los sistemas UNIX (www.nongnu.org/tiger).

Almacenar los registros de forma segura: los **logs** o **registros** de nuestros sistemas deben ser almacenados de forma segura y en un servidor remoto. De esta forma, podremos realizar varios análisis que nos ayudarán a determinar el estado de nuestra infraestructura y los sucesos relacionados con ella.

Crear copias de respaldo regularmente: como todo dato puede sufrir daños totales o parciales, es necesario implementar una política de copias de seguridad, y las herramientas adecuadas para llevarla a cabo.



Figura 8. MBSA es una herramienta que nos permite analizar rápidamente la seguridad de los productos Microsoft (<http://technet.microsoft.com/en-US/security/cc184924.aspx>).



HARDENING EN ORGANIZACIONES



En las organizaciones, el proceso de hardening debe estar perfectamente documentado y estandarizado para que a cada dispositivo se le apliquen las mismas medidas de seguridad. Esto es importante porque cada medida de seguridad que implementemos podría no tener solo resultados positivos, sino también producir un mal funcionamiento en los sistemas y las aplicaciones relacionadas. Además, es preciso tener mucho cuidado al modificar las políticas de hardening que implementamos, y verificar que cada cambio funcione de la forma en la que esperamos. Si es posible, tenemos que utilizar equipos de prueba.



Network Access Control

El **NAC** (*Network Access Control*) unifica tecnologías como antimalware, prevención de intrusos y análisis de vulnerabilidades. Esto nos permite implementar varios controles sobre los dispositivos que están conectados a la red, tanto de preadmisión como de postadmisión, para decidir qué dispositivos pueden conectarse y a qué recursos de red pueden acceder.

Esta tecnología se encuentra en constante evolución, y es implementada de diversas formas por varios fabricantes, que agregan diferentes funcionalidades a cada uno de sus productos. En los sistemas Microsoft Windows, encontramos una implementación llamada **Network Access Protection (NAP)**, que apareció en los sistemas Windows Server 2008. Por su parte, **Cisco Systems** desarrolló una denominada **Network Admission Control**.



Figura 9. PacketFence es un software de código abierto que nos permite implementar NAC en nuestra red (www.packetfence.org).

En la mayoría de los casos, el funcionamiento de esta tecnología se logra a través de un trabajo conjunto entre los servicios DHCP, DNS y los dispositivos de telecomunicaciones. Esto permite ubicar los dis-



positivos que no cumplen con la política de seguridad en una red de cuarentena, y remediar su situación instalando el software antimalware necesario e implementando las configuraciones requeridas por el administrador de la red.

Así como en el caso de la tecnología NIDS, la implementación de un sistema NAC es un proceso complejo, pero que puede ayudarnos a aumentar en gran medida la seguridad de nuestra infraestructura. Pero, a diferencia de los sistemas NIDS, la tecnología NAC está formada por varios componentes distintos, y debemos tener ciertas consideraciones con este tipo de proyectos:

- **Caídas de servicio:** estos sistemas podrían denegar el acceso a la red a dispositivos que deberían acceder normalmente.
- **Cambios necesarios:** es muy habitual que sea necesario realizar modificaciones en la infraestructura para implementar estas tecnologías. Debemos analizar cuidadosamente el costo que podrían llegar a tener estos cambios.
- **Alineamiento a futuro:** es preciso considerar que estas tecnologías nos permitirán hacer evolucionar nuestra infraestructura, pero también, restringirán el modo en que esta puede hacerlo. Debemos considerar si el sistema NAC seleccionado nos permitirá crecer de acuerdo con nuestros planes.

IMPLEMENTAR UN
SISTEMA NAC ES
COMPLEJO PERO
AUMENTA LA
SEGURIDAD



Con la nueva tendencia de los dispositivos móviles, como teléfonos inteligentes y computadoras portátiles, es muy común que los equipos que se conectan a nuestra infraestructura vengan de haberse conectado a varias redes, que pueden haberlos infectado. Por otra parte, este tipo de equipos requiere más control por parte de los usuarios, por lo que se les permite modificar cierto tipo de configuraciones, que podrían llegar a representar riesgos para la seguridad.



Figura 10. En la imagen podemos ver la solución de NAC ofrecida por el fabricante **Sophos** (www.sophos.com).

Malware

El **malware** es todo aquel software desarrollado con el objetivo de producir algún mal en el sistema sin el consentimiento de su propietario. Esta es una descripción muy general, que engloba a una gran cantidad de subtipos de software. Entre los más importantes podemos encontrar **virus**, **gusanos**, **rootkits**, **troyanos**, **spyware** y **keyloggers**.

En particular, la mayoría del malware desarrollado busca atacar sistemas operativos Windows.

En caso de que nuestra organización cuente con pocos dispositivos, podemos optar por instalar alguna de las soluciones gratuitas que se ofrecen en el mercado. La mayoría provee capacidades de detección básicas, y no cuenta con la posibilidad de gestionarse en forma remota, aunque esto es algo que no nos preocupa si debemos proteger una pequeña cantidad de servidores y estaciones de trabajo.

Si nuestra organización cuenta con un gran número de dispositivos, debemos elegir una solución antimalware paga. En este caso, deberemos evaluar con mucho cuidado tanto las capacidades de detección, como el soporte y la interfaz de gestión centralizada que provee el fabricante. Estos tres factores son fundamentales al momento de seleccionar una solución de este tipo.

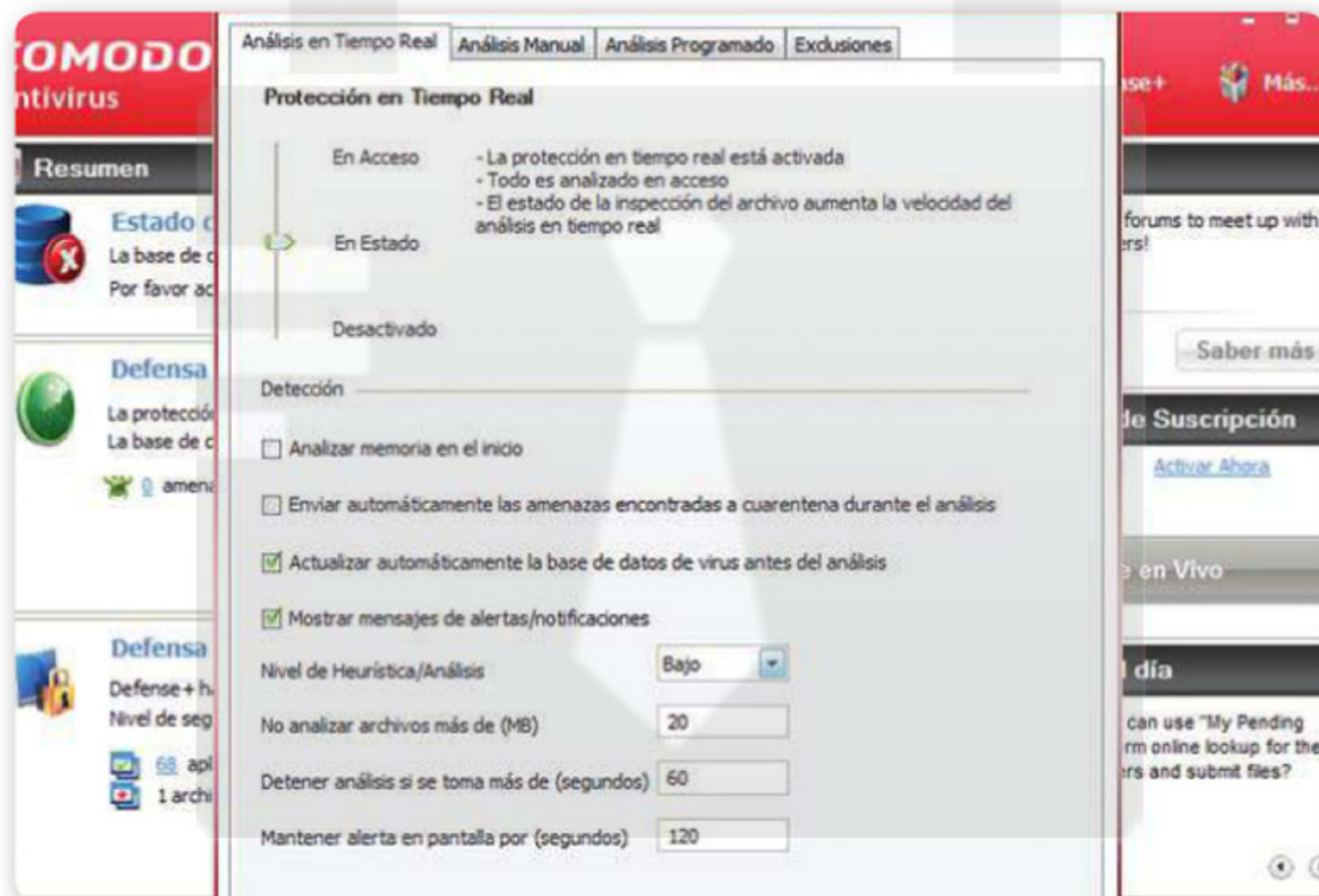


Figura 11. La empresa **Comodo** ofrece software gratuito para la protección contra malware (www.comodo.com).



¿TE RESULTA ÚTIL?

Lo que estás leyendo es el fruto del trabajo de cientos de personas que ponen todo de sí para lograr un mejor producto. Utilizar versiones "pirata" desalienta la inversión y da lugar a publicaciones de menor calidad.

NO ATENTES CONTRA LA LECTURA. NO ATENTES CONTRA TI. COMPRA SÓLO PRODUCTOS ORIGINALES.

Nuestras publicaciones se comercializan en kioscos o puestos de voceadores; librerías; locales cerrados; supermercados e internet (usershop.redusers.com). Si tienes alguna duda, comentario o quieres saber más, puedes contactarnos por medio de usershop@redusers.com

También debemos tener en cuenta que una de las medidas más importantes para luchar contra el malware es la capacitación de los usuarios. Si ellos entienden que no deben ejecutar programas en los cuales no confíen, y que deben evitar la navegación por sitios web de dudosa reputación, los ataques por malware que sufrirá la empresa se verán disminuidos en gran medida.

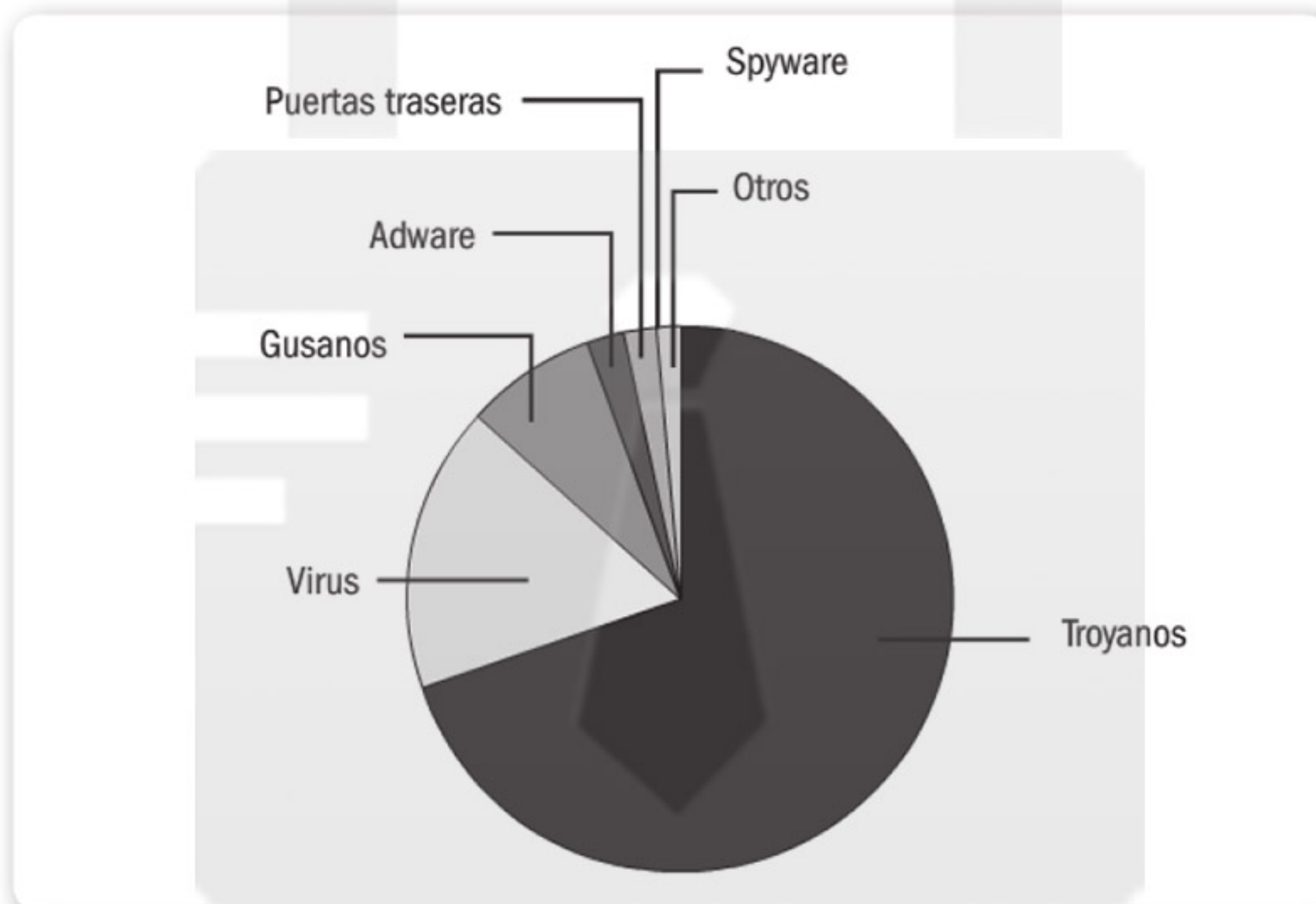


Figura 12. El gráfico muestra estadísticas sobre la clase de malware que se encuentra en internet. La mayoría, son troyanos.



FILTROS DE NAVEGACIÓN



Además del software antimalware, existen otras medidas que podemos tomar para reducir el riesgo de infecciones. Por ejemplo, podemos implementar filtros de navegación web que bloqueen el acceso a sitios sospechosos. Mucho del malware existente se aloja en sitios de descargas gratuitas, pornografía, juegos online y otros similares.



Protección en capas

Como analizamos en capítulos anteriores, el concepto de defensa en profundidad nos permite aumentar enormemente la seguridad de nuestros sistemas al implementar varias capas de defensa. En el caso del malware, esto puede llevarse a la práctica implementando varios controles en diferentes puntos de la red. Por ejemplo, podemos contar con:

- Un dispositivo UTM que se encargue de analizar todo el tráfico que entra y sale de la conexión a internet.
- Un software antimalware en el servidor de archivos, que se ocupe de analizar todos los archivos alojados en él.
- Un software antimalware en cada estación de trabajo.

Con estas tres capas de protección, correctamente administradas y actualizadas, se vuelve casi imposible que un software malicioso consiga ingresar en nuestra infraestructura.

También debemos tener en cuenta que, si bien cada una de estas capas es importante, pueden darse casos particulares en los que una sola tenga que hacer todo el trabajo. Por ejemplo, los virus que se alojan en un pendrive USB podrían ser detectados únicamente por el sistema antimalware de la estación de trabajo correspondiente. Por esta razón, es de vital importancia que cada una de las medidas de seguridad se encuentre en perfecto estado.



Firewalls

Actualmente, todos los sistemas operativos cuentan con sistemas de firewall, ya sea para servidores o para estaciones de trabajo. Tanto **Windows Firewall** (sistemas Windows), como **IPTables** (sistemas GNU/Linux) y **PF** (sistemas OpenBSD) son excelentes herramientas para bloquear los puertos de nuestros sistemas a los que se puede acceder desde la red. En el caso de las plataformas Microsoft, podemos encontrar varias soluciones que intentan reemplazar al firewall incluido en forma

predeterminada. En este caso, deberemos analizar qué ventajas y desventajas podría traernos implementarlas.

En los sistemas Windows, es posible realizar excelentes configuraciones a través de Active Directory, para mantener un estándar de puertos permitidos. Con esto nos aseguramos de bloquear algunos de los ataques más comunes realizando un esfuerzo mínimo.

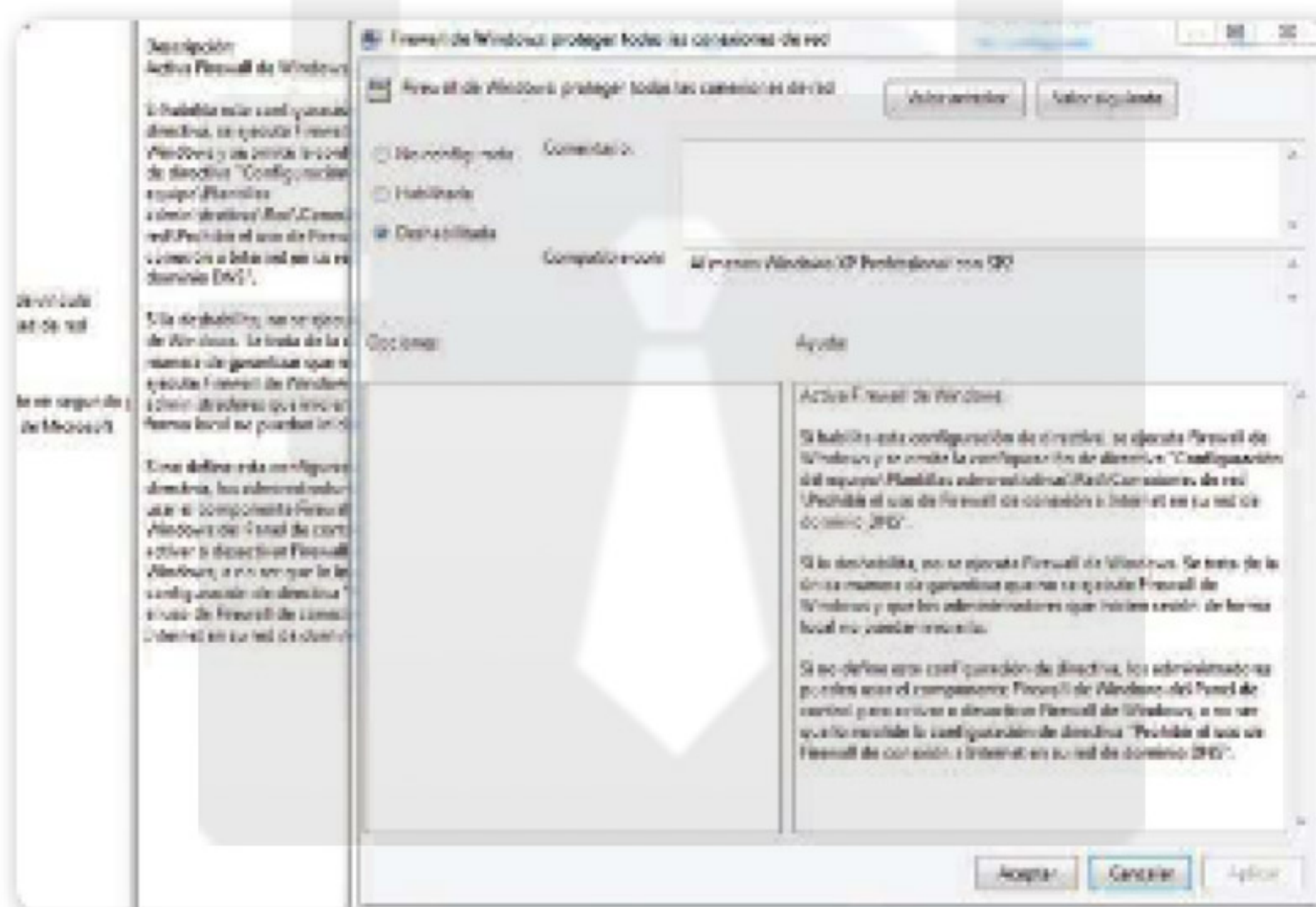


Figura 13. Aquí vemos cómo podemos configurar el firewall de Windows a través de Group Policies.

Debemos considerar la implementación de firewalls en las estaciones de trabajo como medida de seguridad opcional, y analizar cuánto trabajo puede llevarnos mantener las reglas de filtrado de cada sistema, con respecto al beneficio de seguridad que nos representa.

En la mayoría de los casos, deberemos optar por implementar una misma configuración para todas las estaciones de trabajo, con el fin de simplificar la gestión de reglas, aunque esto haga que nuestra configuración diste de ser perfecta.



Figura 14. ZoneAlarm es una excelente alternativa al firewall de Windows, lo encontramos en www.zonealarm.com.

Cuando nos referimos a estaciones de trabajo, generalmente no necesitamos que haya puertos abiertos. Por lo tanto, podemos optar por cerrar todos los puertos, salvo los de administración remota. En el caso de los servidores, debemos permitir únicamente las conexiones a los puertos de servicio, y solo desde los equipos que tienen motivo para conectarse.



Backups

La mayoría de nuestros servidores (por no decir todos) tendrán alguna información que debería ser resguardada por si algo malo llegara a suceder. Y, cuando hablamos de algo malo, debemos considerar varias posibilidades, como fallas de discos, errores de usuario, ataques de malware, y otras acciones. Es por eso que la realización de copias de seguridad es una tarea

prácticamente obligatoria en todos los casos. Solamente debemos pensar en la cantidad de datos por respaldar, la frecuencia de respaldo y el tiempo durante el cual vamos a almacenar las copias antes de eliminarlas.

Tanto si vamos a realizar copias de bases de datos, como de configuraciones, correos electrónicos u otros archivos, el uso de herramientas específicas nos simplificará la tarea de manera notable. Por esta razón, una de nuestras primeras decisiones cuando pensamos en respaldar los datos es seleccionar cómo lo haremos. Para esto, podemos optar por herramientas pequeñas, diferentes para cada sistema operativo; o por herramientas grandes, que se adaptan a cualquier entorno. Esta es una decisión que depende más de gustos que de necesidades.

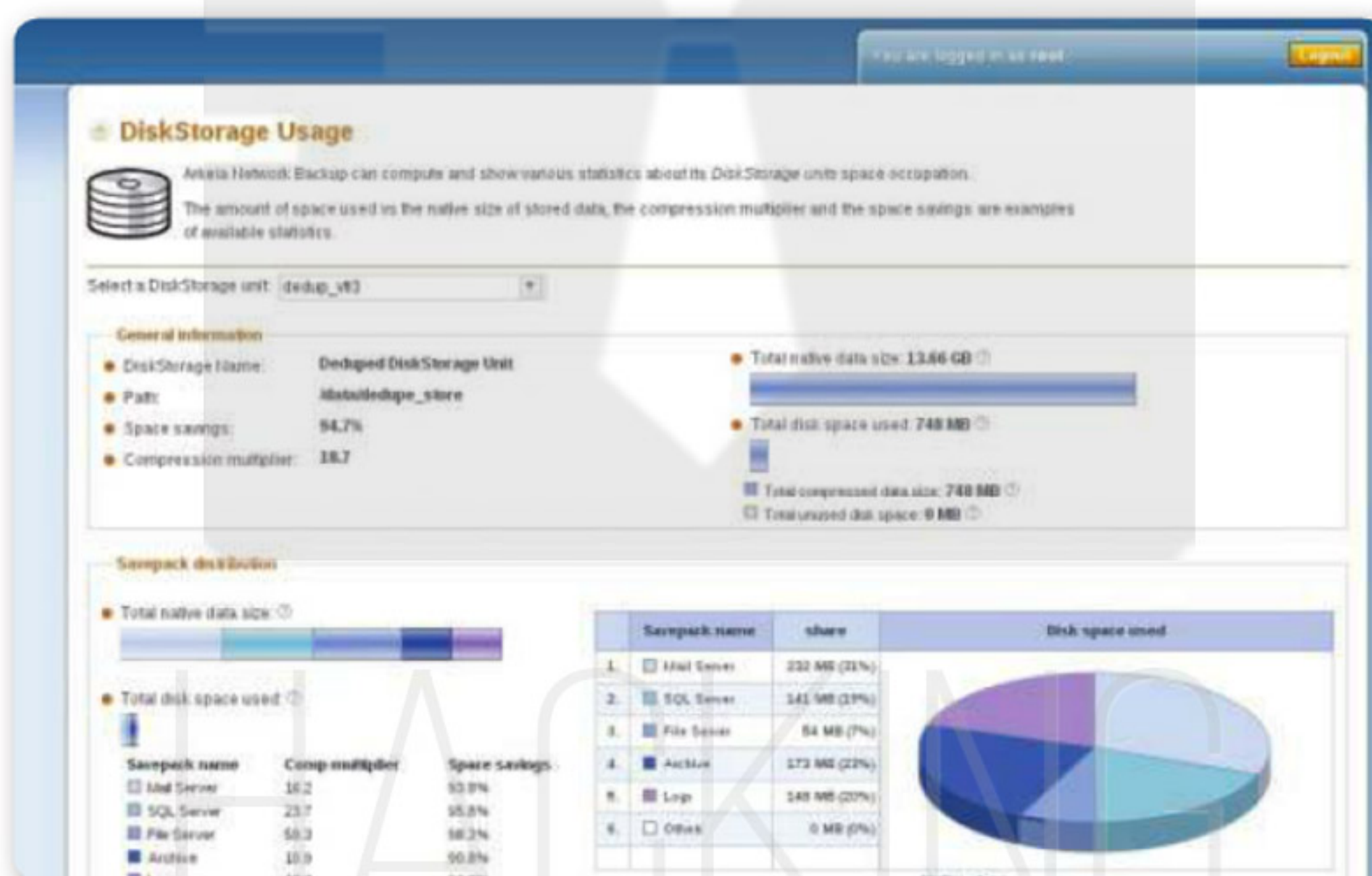


Figura 15. El fabricante **Arkeia** cuenta con una gran cantidad de productos para el resguardo y la recuperación de datos (www.arkeia.com).

Herramientas basadas en agentes

Muchas herramientas del mercado que están basadas en la arquitectura cliente/servidor utilizan agentes instalados en cada uno de los disposi-

tivos de los cuales vamos a hacer copias de seguridad. Esto suele darles más control sobre los parámetros que se van a configurar, y permite que el agente realice tareas como compresión y encriptación de datos. En estos casos, son los agentes los que se conectan con el servidor principal para efectuar la transferencia de datos.

Herramientas sin agentes

Existen otras herramientas en las que el servidor realiza las conexiones cuando se van a generar los respaldos. Estas conexiones, por lo general, se hacen a través de interfaces de administración, como SSH, RPC o SNMP. Debemos considerar que estas herramientas suelen ser menos flexibles, pero no están limitadas a los sistemas operativos para los cuales se haya desarrollado un agente.

Scripts personalizados

Los grandes aliados de todo administrador de sistemas son los scripts personalizados que realizan tareas puntuales; por ejemplo, hacer una conexión a través de SSH, crear un archivo comprimido con todos los datos que se necesita respaldar, encriptarlo y transferirlo a través del protocolo FTP a otro servidor. Sin dudas, podemos sacar gran provecho de la implementación de este tipo de herramientas, que son pequeñas pero muy potentes.

Por ejemplo, con el código que se presenta a continuación, podemos, desde GNU/Linux, realizar una copia de las bases de datos MySQL de cualquiera de nuestros servidores:

```
#!/bin/bash  
USER=usuario  
PASS=clave
```



```
for db in `echo "show databases" | mysql -u$USER -p$PASS | grep -v ^mysql$ |  
grep -v ^Database$`;  
do  
    mysqldump --add-drop-table --routines -u $USER -p $PASS ${db}> ${db}.sql;  
  
done
```

Recuperación completa

Existen herramientas desarrolladas con el objetivo de recuperar un sistema completamente, es decir, tanto el sistema operativo como los datos y las configuraciones. Esto se logra creando una imagen del contenido de los discos de almacenamiento. Este tipo de herramientas suele llamarse de **clonado de discos** o de **recuperación de desastres**, porque, en general, se utilizan en última instancia, cuando todo el sistema se encuentra inoperable. También se presentan como alternativas que pueden usarse para realizar instalaciones masivas, tanto de estaciones de trabajo como de servidores.

Es un excelente recurso clonar discos para instalar automáticamente estaciones de trabajo preconfiguradas de forma segura.



AGENTES Y SCRIPTS



Existe un tercer tipo de herramienta, aún más completa, que puede utilizar agentes, pero que, en caso de que estos no estén disponibles, puede realizar conexiones a puertos de administración o ejecutar scripts personalizados. Estas herramientas son las más flexibles, y deberían ser nuestra opción si nuestra infraestructura es compleja.





Autenticación multifactor

Para las conexiones a servicios críticos, podemos utilizar lo que se conoce como **autenticación multifactor**. En este caso, le solicitamos al usuario que se identifique no solo con una contraseña, sino también con algo que tiene en su poder, como una llave USB. Este es un concepto muy relacionado con el de **defensa en profundidad**, en el cual implementamos varias medidas de seguridad para proteger nuestros activos de información.

A continuación, analizaremos algunos de los factores de autenticación más utilizados.

Tokens o smart cards

Estos dispositivos electrónicos, básicamente, presentan una clave adicional que se genera en forma dinámica y aleatoria, y permite demostrar que el usuario se encuentra en posesión del dispositivo al momento de ingresar sus credenciales. Existen varios tipos de métodos para lograr este fin, pero, en principio, todos cumplen con la misma función.



Figura 16. Podemos ver **tokens SecureID**, desarrollados por RSA, que muestran ejemplos de los valores aleatorios generados.

Tokens virtuales

Los tokens virtuales buscan ser una alternativa más económica que los tradicionales, esto es así porque se recurre a un dispositivo que el usuario ya posee. Esto suele lograrse con la instalación de un software en una laptop o teléfono celular del usuario, que cumple con funciones similares a las de un token tradicional. Si bien puede discutirse que el nivel de seguridad en este caso es inferior al de los tokens tradicionales o smart cards, estos son una excelente alternativa para aquellos casos en que nuestros recursos económicos son escasos.



Figura 17. Mobile-OTP permite a los teléfonos celulares trabajar como dispositivos de **token virtual** (<http://motp.sourceforge.net>).

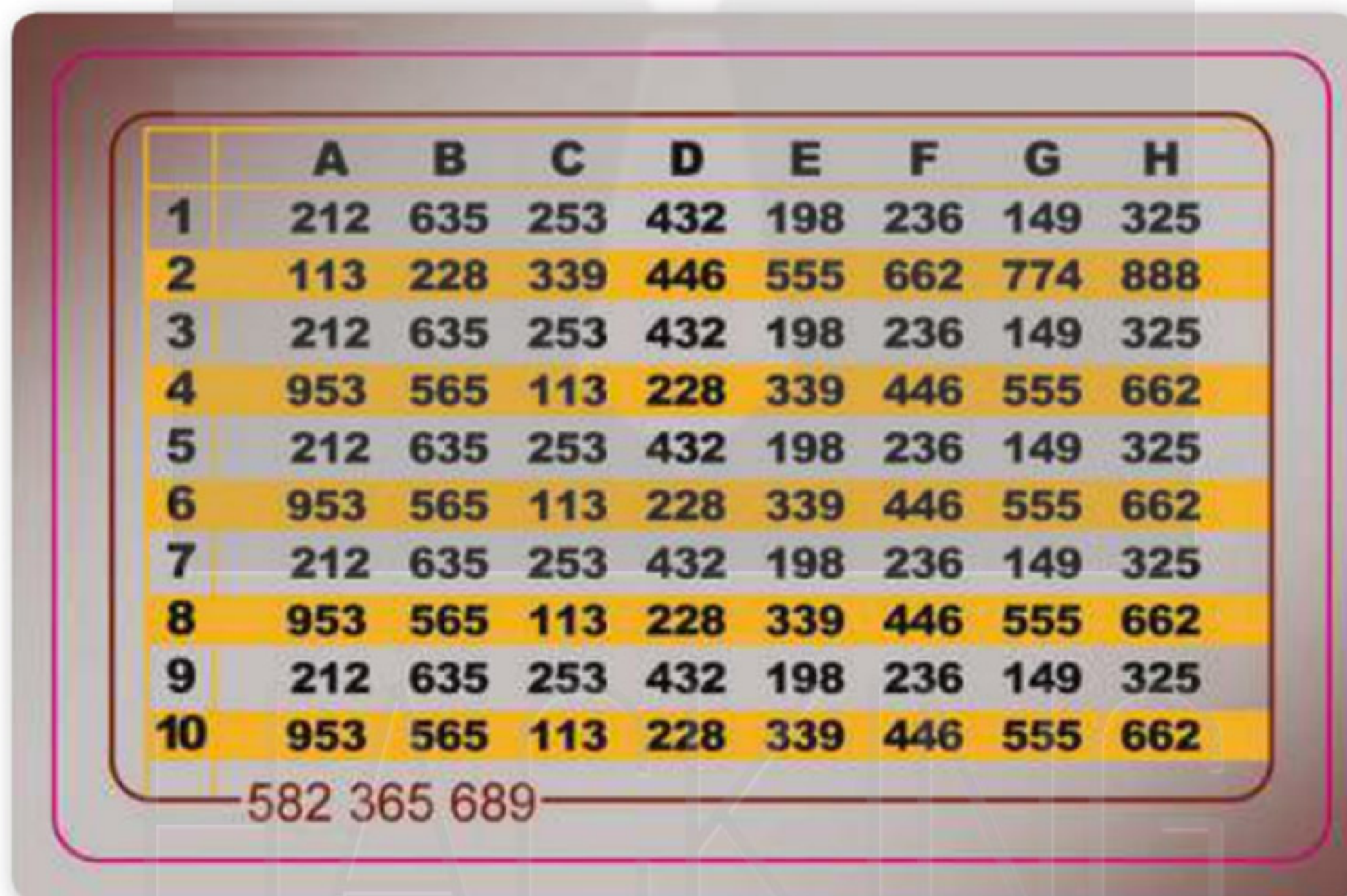
Tarjetas de coordenadas

Una opción aún más económica se logra por medio de tarjetas que tienen una serie de filas y columnas, en las que cada combinación de fila/columna representa un código único. Al momento de autenticar al usuario, se le solicita a este que ingrese el valor, por ejemplo, de **Fila A - Columna 10**.

La principal ventaja de este método es que las tarjetas pueden ser generadas automáticamente por un servidor, y distribuidas por medios electrónicos seguros (como un correo electrónico cifrado). Esto resulta en un costo prácticamente nulo.

Aunque debemos considerar que es el método más inseguro de todos, por varias fallas que podrían asociarse a esta técnica, podemos decir que es mucho mejor que utilizar autenticación simple. Junto con los tokens, es un método muy empleado en el sector bancario para realizar transferencias electrónicas de dinero.

Es mejor implementar una buena medida de seguridad económica, que no implementar una excelente medida de seguridad costosa.



	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	113	228	339	446	555	662	774	888
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	953	565	113	228	339	446	555	662
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662
582 365 689								

Figura 18. En la imagen podemos ver un ejemplo de una tarjeta de coordenadas utilizada por un banco para la autenticación de sus clientes.

Biometría

Esta tecnología se encarga de verificar la identidad del usuario comprobando factores que estén relacionados con la biología de la persona (de

ahí el nombre, **biometría**). Algunas de las características más utilizadas son: escaneo de iris, escaneo de retina y escaneo de huellas dactilares.

Estos métodos tienen un alto porcentaje de fiabilidad, aunque poseen la desventaja de que los lectores tienen un costo relativamente elevado y no son muy portables, por lo que, generalmente, se utilizan para accesos físicos y no tanto para accesos remotos.



Figura 19. Podemos ver un dispositivo que escanea huellas digitales y permite ingresar una clave numérica para controlar un acceso físico.



WIKID



La empresa WikID Systems ha desarrollado un software de servidor para autenticaciones multifactor, que cuenta con clientes para Windows, Mac, Linux, Blackberry, Palm, Windows Mobile and J2ME. Tiene una versión de código abierto y otra comercial, que ofrece una mayor cantidad de funcionalidades (www.wikidsystems.com).





Servidores de autenticación

La administración de perfiles de usuario es otra de las tareas de importancia crítica para la seguridad informática, porque se encarga de definir quién, cómo y cuándo puede acceder a los sistemas. Es por eso que siempre debemos optimizar este tipo de tareas y las tecnologías que están relacionadas con ellas.

Al contar con un servidor que almacene la información de usuarios, grupos y perfiles, podemos determinar a qué servicios puede acceder una persona directamente modificando sus atributos.

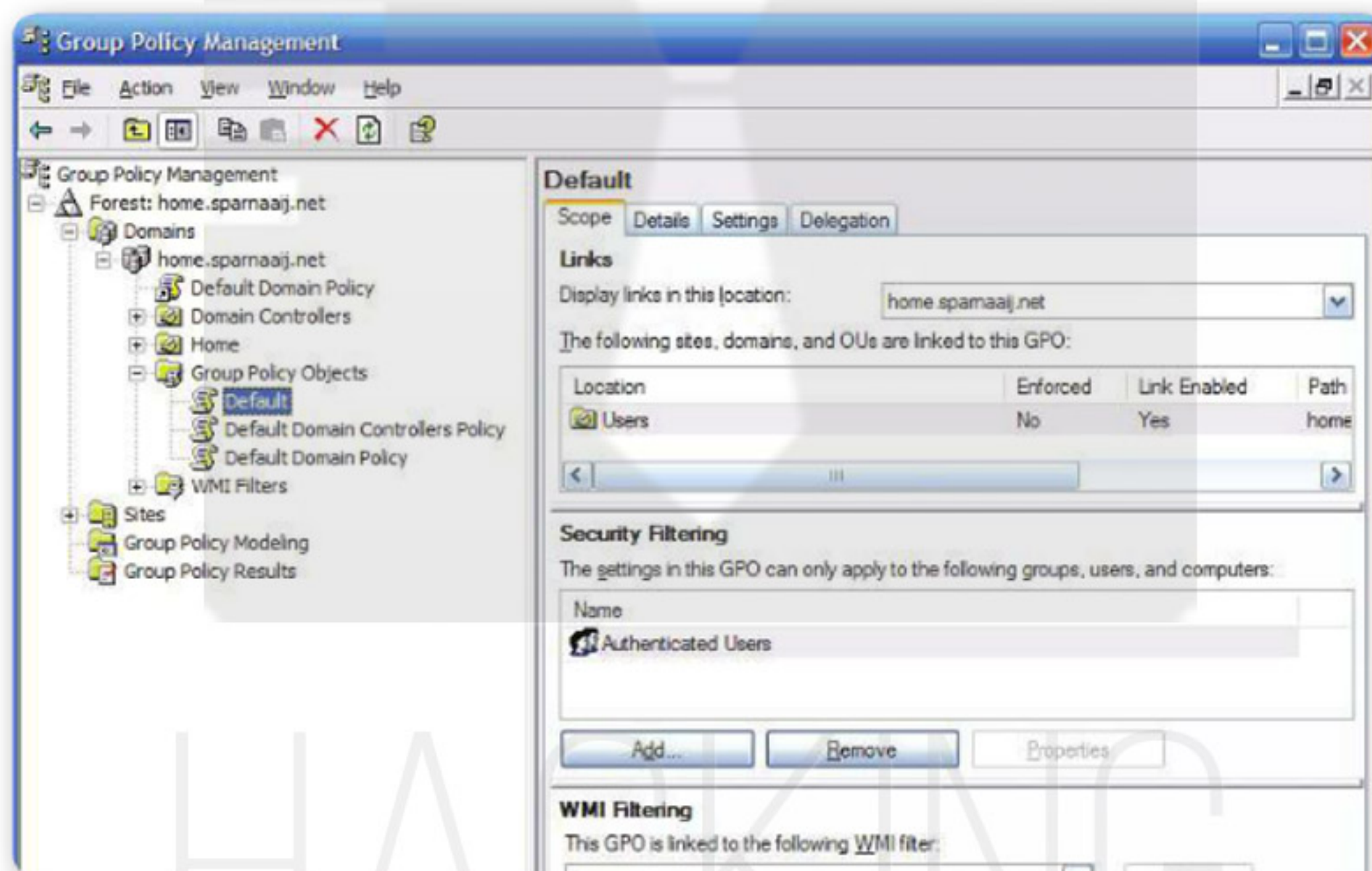


Figura 20. Las **Group Policies** de **Active Directory** nos permiten definir múltiples opciones de seguridad para nuestros equipos Windows.

Existen varias tecnologías que nos permiten implementar un servidor de autenticación centralizada, cada una, con sus respectivas ventajas y desventajas. Actualmente, las implementaciones más populares están basadas en el **protocolo LDAP**, que es una especie de base de datos que agrupa los registros en un formato de árbol.

El producto más implementado actualmente es Active Directory (desarrollado por Microsoft), pero también hay otros, tanto comerciales como de código abierto. En el caso de los productos de código abierto, podemos destacar a **OpenLDAP**, **FreeIPA** y **Mandriva Directory Server**.

Active Directory ofrece una integración muy fuerte con los clientes y servidores Windows, que nos permite implementar varias políticas de seguridad y plantillas de configuraciones. Esto hace que, desde un único lugar, tengamos la posibilidad de implementar configuraciones, establecer políticas y distribuir software.

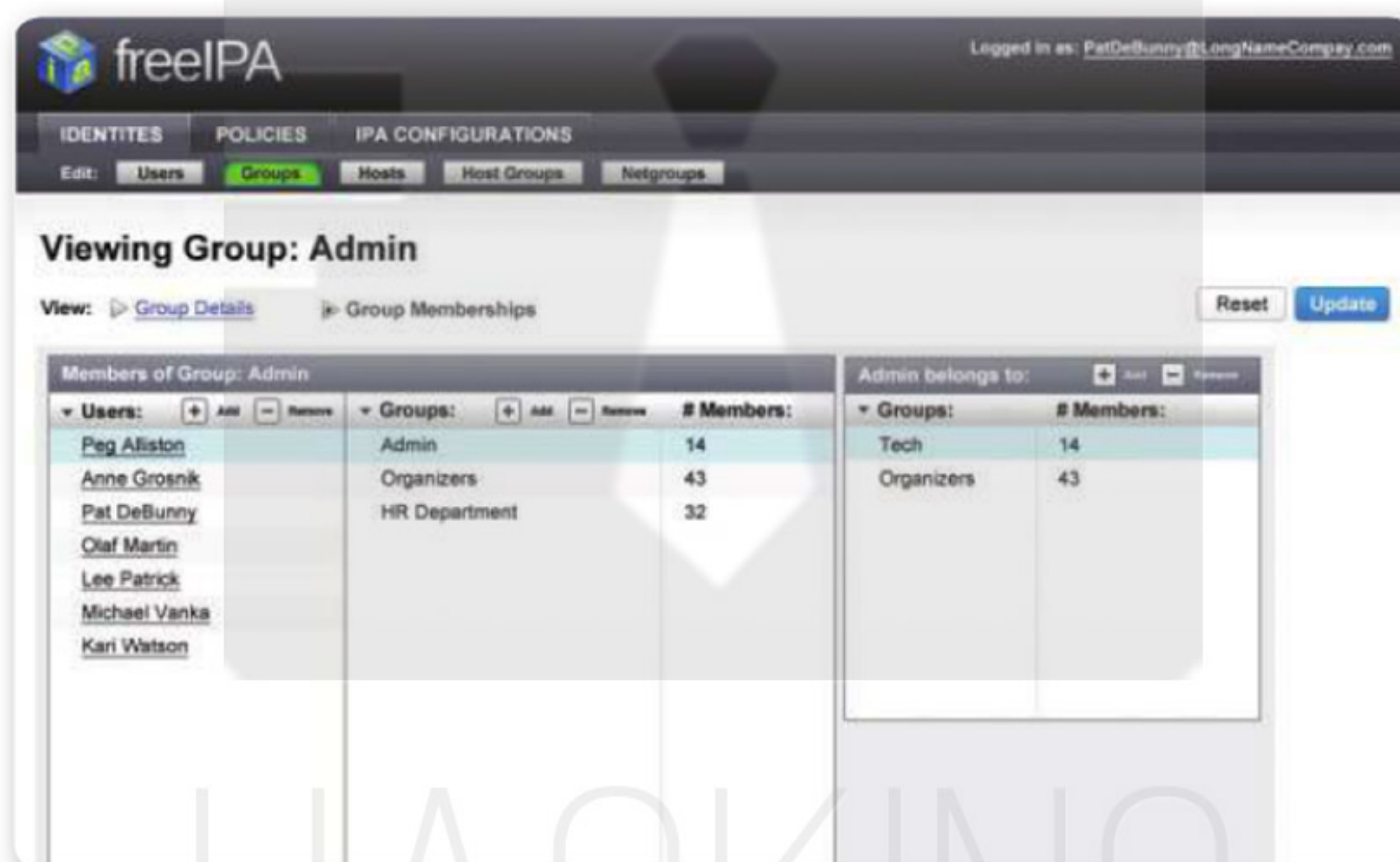


Figura 21. El proyecto **FreeIPA** ofrece una solución libre para la gestión de identidades (<http://freeipa.org>).

Los servidores de autenticación nos permiten centralizar no solamente las credenciales de acceso para nuestras estaciones de trabajo y servidores, sino también los accesos de nuestros dispositivos de telecomunicaciones. En el caso de Active Directory, podemos habilitar el protocolo Radius utilizando los mismos datos de cuentas que se encuentran en la base de datos LDAP del producto. Todas las soluciones de autenticación centrali-

zada tienen la posibilidad de brindar varios métodos de autenticación.

La mayoría de los accesos no autorizados suceden a través de cuentas de acceso autorizadas. Si las mantenemos controladas, habremos dado un paso importante.

LOS ACCESOS NO
AUTORIZADOS
SE REALIZAN
DESDE CUENTAS
AUTORIZADAS

Análisis de logs

El almacenamiento y análisis de registros (o **logs**) es una de las tareas más importantes en lo que a la seguridad informática se refiere. Muchas herramientas de seguridad están basadas en el análisis de este tipo de registros, y nos permiten conocer estadísticas y sucesos sospechosos, lo cual nos da la posibilidad de analizar tendencias y deducir comportamientos futuros. Además, debemos considerar que los atacantes siempre intentarán eliminar los registros en los sistemas en los que hayan podido penetrar, a fin de borrar las huellas del ataque.

Otro aspecto importante del análisis de logs es que puede ser utilizado no solamente para conocer los eventos pasados, sino también para proyectar los eventos futuros. Este es un aspecto clave, porque un análisis detallado de los logs nos permitirá tomar decisiones acertadas acerca de qué medidas de seguridad implementar o reforzar. Es por este motivo que resulta fundamental contar con un servidor centralizado, en el cual podamos almacenar todos los registros de nuestros sistemas.

Una de las tantas diferencias que existen entre los sistemas operativos Windows y UNIX es el formato de logs utilizado en cada caso: **syslog** es el más empleado en UNIX (también utilizado en la mayoría de los dispositivos de telecomunicaciones), mientras que **EventLog** es el que emplean las plataformas Microsoft.

Es importante realizar la unificación de este tipo de logs, y también implementar una herramienta que nos permita gestionar y analizar todos los datos en un único lugar.



Figura 22. EventLog Analyzer nos permite centralizar los logs tanto en formato **syslog** como **EventLog** (www.manageengine.com).

Servidores centralizados

Para poder realizar un verdadero análisis de los logs de nuestros dispositivos, es necesario que estos se encuentren centralizados en un único lugar. Esto, además, nos permitirá hacer una correlación de los datos, de



METODOLOGÍA

Ya sea a través de herramientas complejas o de pequeños scripts realizados en algún lenguaje como Perl o Python, debemos implementar alguna metodología de análisis de logs. Esto nos permitirá simplificar nuestras tareas, realizar análisis en tiempo real, recibir notificaciones y contar con una mejor comprensión de nuestra infraestructura.



modo que podremos reaccionar no solo ante los eventos ocurridos en un sistema, sino también sobre la base de la relación que existe entre los eventos de varios sistemas.

La correlación de eventos es de suma importancia si verdaderamente queremos tener un control sobre lo que sucede en nuestra infraestructura, porque no siempre podemos obtener toda la información necesaria de un único dispositivo. Por el contrario, a veces necesitamos varias fuentes de información para comprender exactamente qué es lo que está sucediendo.

Debemos prestar mucha atención a configurar correctamente el servidor central, para que los logs se almacenen como corresponda, no puedan ser modificados y se les haga una copia de seguridad en forma regular. También tenemos que considerar que el servidor de logs podría ser nuestro único recurso para analizar las características de un ataque o cualquier otro evento que haya impactado negativamente en la infraestructura.

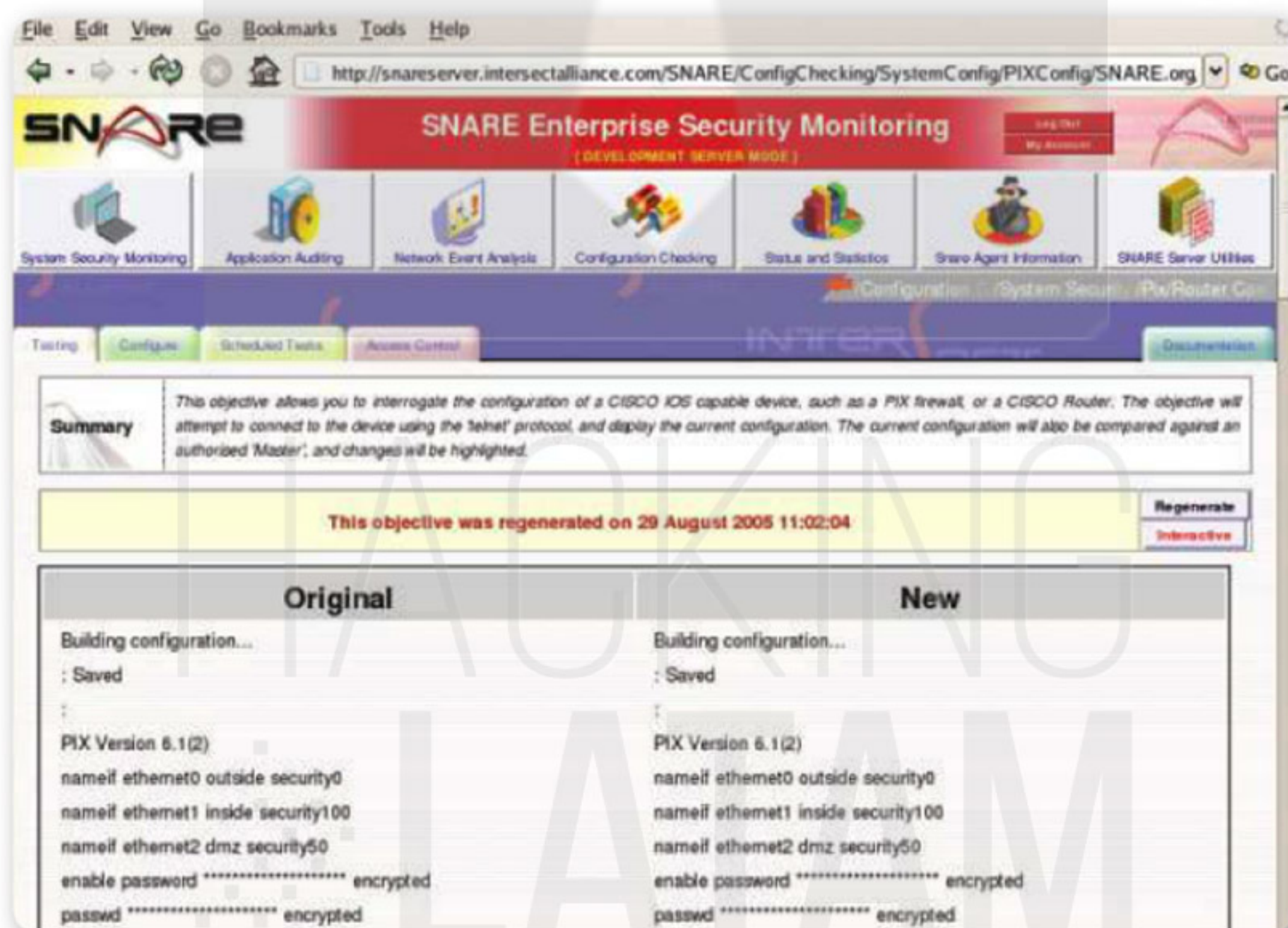


Figura 23. InterSect Alliance desarrolla aplicaciones cuyo objetivo es centralizar y analizar los logs de varios tipos (www.intersectalliance.com).

A continuación, explicamos algunos de los aspectos de seguridad que debemos considerar al implementar un servidor de logs centralizado:

- Los archivos de logs no pueden ser modificados, salvo para eliminarlos cuando haya pasado el tiempo de retención definido.
- Los logs deben ser analizados automáticamente, para generar reportes de fácil comprensión.
- Se debe implementar un sistema de alertas, que notifique a los administradores acerca de sucesos que requieran atención inmediata.

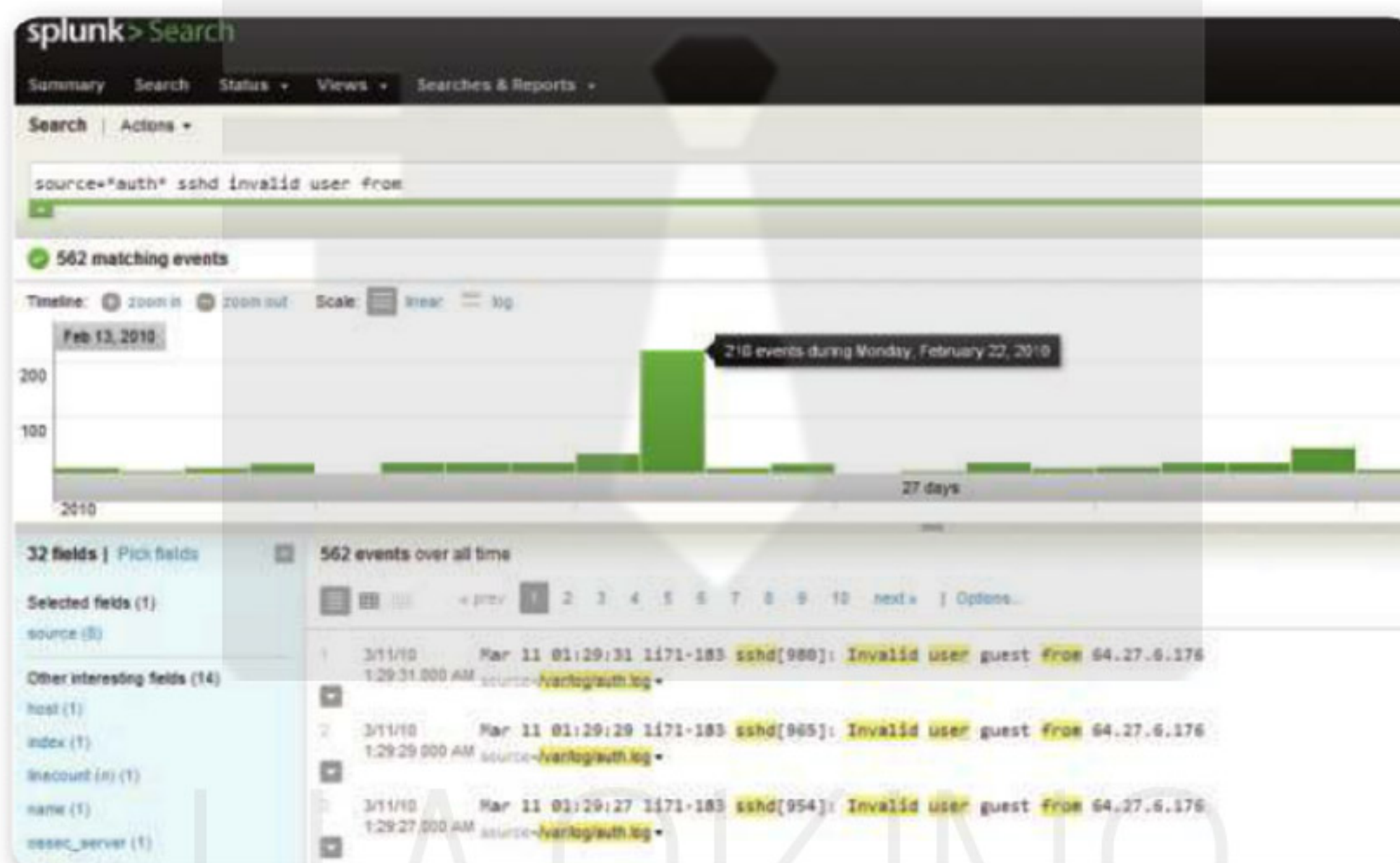


Figura 24. Splunk permite analizar varios tipos de datos, con el objetivo de saber todo lo que sucede en nuestra red (www.splunk.com).



Administración remota

Las herramientas de administración remota son utilizadas, normalmente, para gestionar los servidores y otros dispositivos sin tener nece-

sidad de acceder físicamente a ellos. Esta comodidad es casi necesaria, pero debemos tomar los recaudos de seguridad apropiados al implementar estas tecnologías.

Gracias a este tipo de herramientas, podemos tanto simplificar nuestras tareas y optimizar nuestro trabajo, como abrir grandes vulnerabilidades en los sistemas. Es por eso que debemos planificar correctamente la implementación de herramientas y protocolos de gestión remota. Algunas de las consideraciones para tener en cuenta son comunes para todas ellas, como buenas políticas de autenticación, encriptación de datos, etcétera.

De ser posible, debemos seleccionar una misma herramienta de gestión para todos los dispositivos o, por lo menos, una herramienta para cada tipo de plataforma (por ejemplo, UNIX, Windows y Cisco).

Port knocking

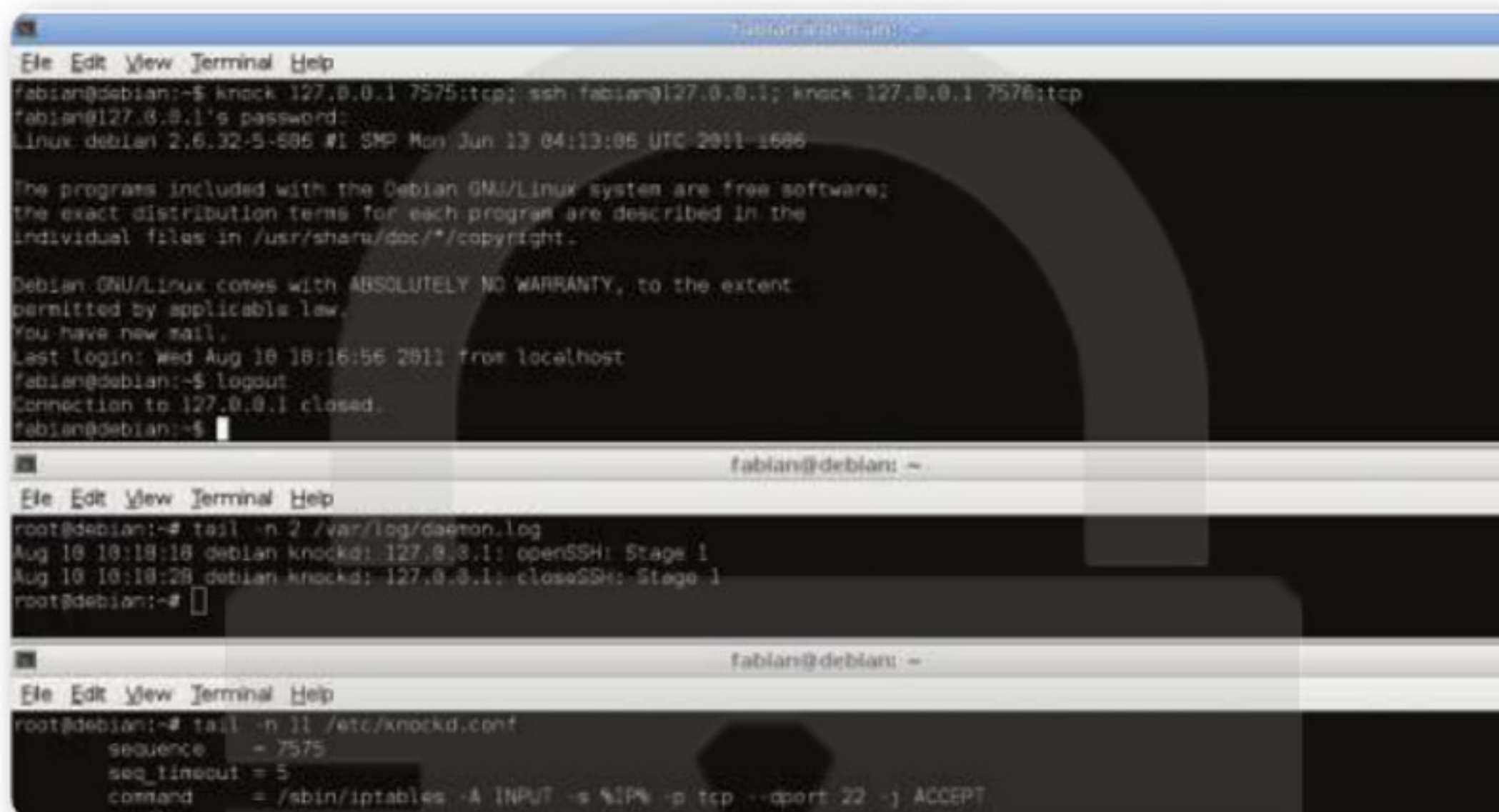
Se trata de un mecanismo para abrir puertos externamente en un firewall mediante una secuencia preestablecida de intentos de conexión a aquellos que están cerrados. Una vez que el firewall recibe una secuencia de conexión correcta, sus reglas son modificadas para permitir que el host que realizó los intentos se conecte a un puerto específico.

Si bien la idea no ha sido puesta en práctica en una gran cantidad de organizaciones, representa una excelente opción cuando necesitamos dejar un acceso externo hacia nuestros sistemas para casos de emergencia, pero buscamos que dicho acceso esté cerrado la mayor parte del tiempo. Normalmente, se utiliza en conjunto con SSH, para tener acceso a una línea de comandos del algún equipo de nuestra infraestructura.

Es casi imposible que una persona que no conozca la secuencia correcta para abrir un determinado puerto consiga detectar el comportamiento de nuestros sistemas, de modo que es un método realmente seguro para un acceso remoto.

PORT KNOCKING
PERMITE ABRIR
PUERTOS EN
UN FIREWALL
EXTERNAMENTE





```

fabian@debian:~$ knock 127.0.0.1 7575:tcp; ssh fabian@127.0.0.1; knock 127.0.0.1 7576:tcp
fabian@127.0.0.1's password:
Linux debian 2.6.32-5-686 #1 SMP Mon Jun 13 04:13:06 UTC 2011 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Aug 10 18:16:56 2011 from localhost
fabian@debian:~$ logout
Connection to 127.0.0.1 closed.
fabian@debian:~$

root@debian:~# tail -n 2 /var/log/daemon.log
Aug 10 18:18:18 debian knockd: 127.0.0.1: openSSH: Stage 1
Aug 10 18:18:28 debian knockd: 127.0.0.1: closeSSH: Stage 1
root@debian:~#

root@debian:~# tail -n 11 /etc/knockd.conf
sequence      = 7575
seq_timeout   = 5
command       = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

```

Figura 25. Vemos la utilización de **knockd** para implementar una solución de **port knocking** en **sistemas Linux** (www.zeroflux.org/projects/knock).

WMI

Windows Management Instrumentation se presenta como una serie de extensiones que permiten realizar la administración remota de sistemas Microsoft Windows. Es importante tener en cuenta que está basado en los estándares abiertos WBEM y también CIM, los cuales fueron desarrollados por el *Distributed Management Task Force* (DMTF).



SEGURIDAD AVANZADA



Es necesario implementar medidas de seguridad avanzadas, debido a que la mayoría de las organizaciones emplea sistemas que procesan o almacenan su información crítica. Es por eso que se recomienda encarecidamente, por lo menos, realizar un análisis de la criticidad de los sistemas y, sobre esa base, estudiar la posibilidad de implementar tecnologías de autenticación multifactor.



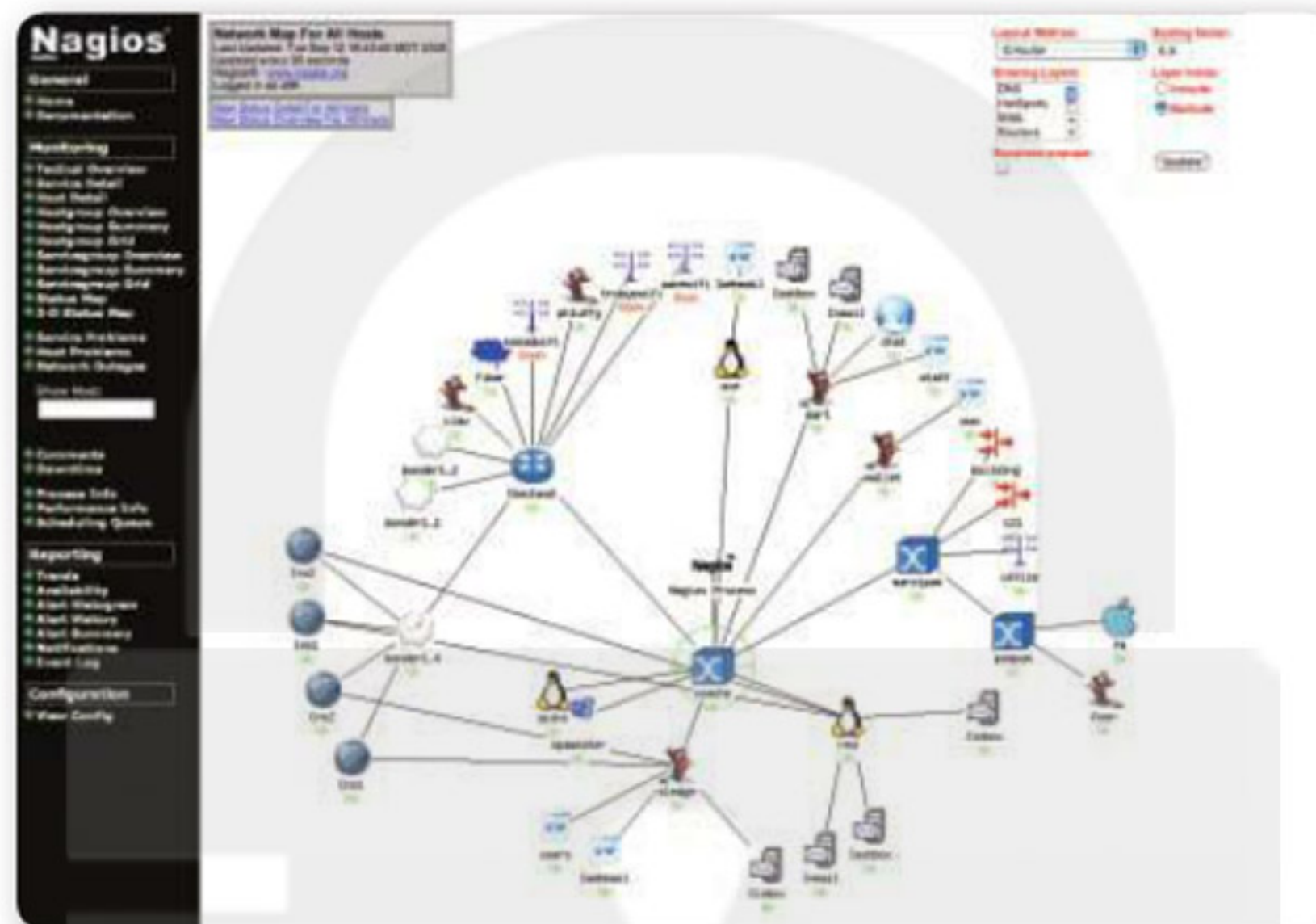


Figura 26. Algunos de los plugins para **Nagios** nos permiten agregar soporte para monitoreo a través de WMI (<http://exchange.nagios.org>).

WIM utiliza la autenticación del propio sistema operativo, que suele ser por base de datos interna o Active Directory, lo que nos permite simplificar la asignación de perfiles, y definir quién puede administrar los equipos y quién no.



Figura 27. **Solarwinds** desarrolla herramientas para el monitoreo de redes, muchas de ellas, con soporte para WMI (www.solarwinds.com).

En el ejemplo que está a continuación, observamos cómo puede utilizarse WMI a través del lenguaje C# para consultar el SSID de la red inalámbrica actualmente conectada:

```
ManagementClass mc = new ManagementClass("root\\WMI", "MSNdis_80211_
    ServiceSetIdentifier", null);
ManagementObjectCollection moc = mc.GetInstances();

foreach (ManagementObject mo in moc)
{
    string wlanCard = (string)mo["InstanceName"];
    bool active;
    if (!bool.TryParse((string)mo["Active"], out active))
    {
        active = false;
    }
    byte[] ssid = (byte[])mo["Ndis80211SsId"];
}
```

**ULTRAVNC**

Una de las implementaciones más populares de código abierto del protocolo VNC para sistemas Windows es **UltraVNC**. Este software cuenta con muchas características interesantes, como autenticación por **Active Directory**, transferencia de archivos, encriptación de datos, y otras. El proyecto ha desarrollado tanto un cliente como un servidor (www.uvnc.com).

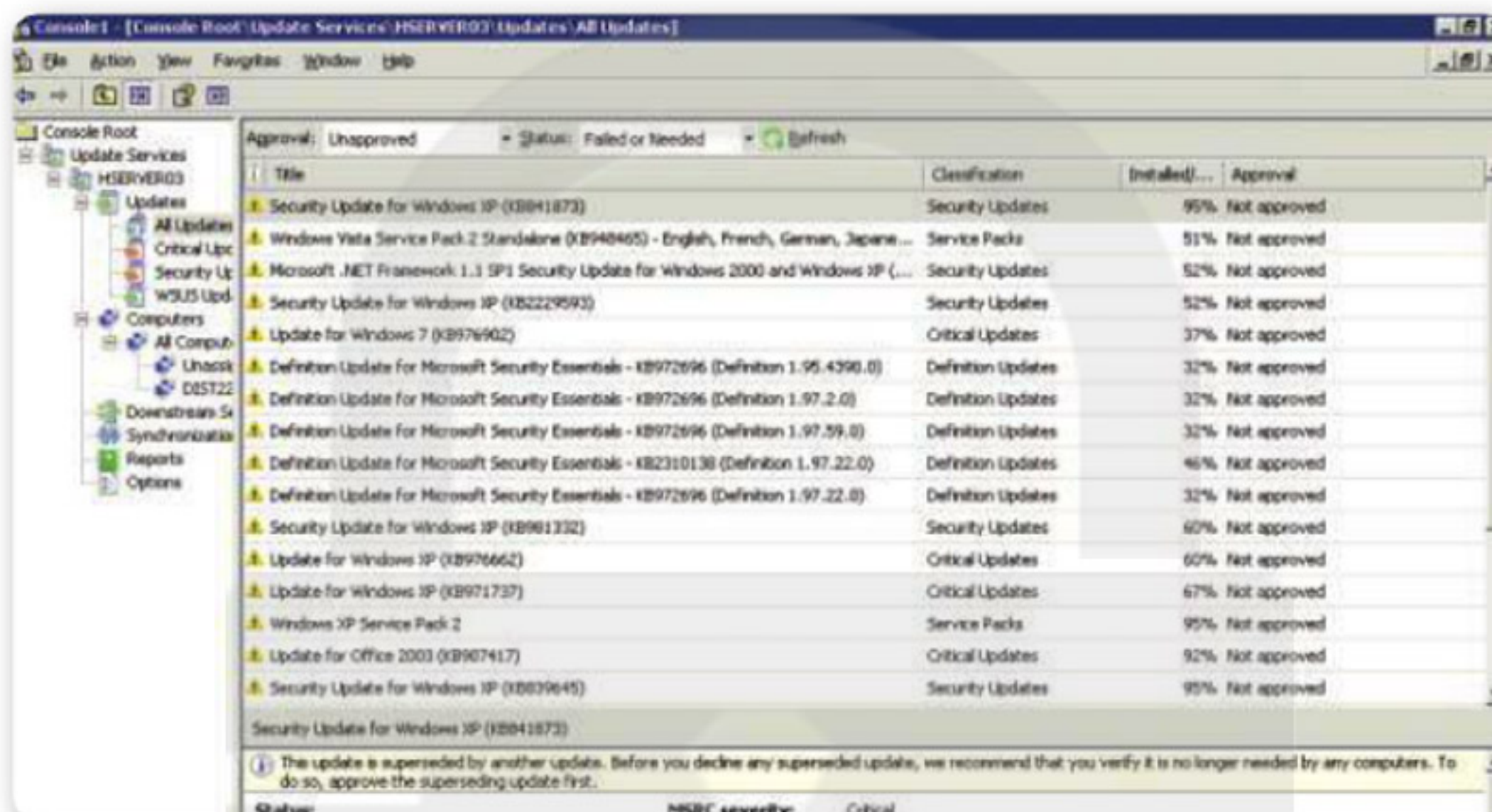


Figura 28. MMC es la herramienta de los sistemas Windows destinada a la administración de usuarios, servicios y otros parámetros.

RDP y VNC

Remote Desktop Protocol y *Virtual Network Computing* son protocolos desarrollados para permitir el acceso remoto a los escritorios, tanto de estaciones de trabajo como de servidores. En ambos casos, existen versiones disponibles para sistemas UNIX y Windows. Si vamos a utilizar este tipo de protocolos, debemos asegurarnos de configurarlos correctamente, para evitar posibles accesos no autorizados.

SSH

Como analizamos en el **Capítulo 4**, el protocolo SSH puede ser utilizado tanto para administrar servidores como para implementar conexiones del tipo VPN o crear túneles para aplicaciones específicas. Es particularmente popular en los sistemas del tipo UNIX.

SSH PUEDE SER
USADO PARA
ADMINISTRAR
SERVIDORES O
IMPLEMENTAR VPN





Figura 29. KTS es un servidor de Telnet y SSH para los sistemas operativos Windows (www.kpym.com).

SNMP

En el **Capítulo 4** también vimos que SNMP puede ser utilizado tanto para consultar como para modificar valores en los sistemas. Si bien su uso es más frecuente en dispositivos de telecomunicaciones, existen versiones para sistemas Microsoft Windows y UNIX.

Webmin

Este software nos permite contar con una **interfaz de gestión web** (WUI) para nuestros sistemas UNIX. Es un proyecto de código abierto que lleva varios años en el mercado y tiene módulos para gestionar infinidad de aspectos del sistema operativo, tanto para las configuraciones básicas de usuarios, almacenamiento, red y firewall, como para los servicios de DNS, DHCP, SMTP y muchos otros. Su implementación puede simplificar de manera notable la gestión de los servidores, permite realizar tareas distribuidas entre varios equipos diferentes y define perfiles de acceso para cada uno de los usuarios. Por lo tanto, es un excelente complemento para otros accesos, como SSH.



Figura 30. En el sitio web de **Webmin** podemos encontrar varios módulos para agregar funcionalidades (www.webmin.com).

Detección de intrusos

Existen diversos tipos de software diseñados para prevenir intrusiones en hosts (*Host-based Intrusion Prevention Systems*, HIPS). Particularmente, hay ciertos factores para observar en un sistema operativo, tendientes a detectar si hemos sido víctimas de una intrusión. Entre ellos, algunos de los más importantes son:

Integridad de archivos: se verifican el tamaño, los permisos, el hash y otros parámetros de cada uno de los archivos del sistema. En caso de encontrar cambios inesperados, estos son reportados.

Monitoreo de registros: se verifican constantemente los archivos de registro (logs), con el objetivo de detectar sucesos extraños o no deseados.

Registro de Windows: en el caso de las plataformas Microsoft, se verifican todas las claves de registro y se analizan los cambios realizados.

Puertos abiertos: se define una configuración que determina qué puertos deben estar abiertos. En caso de producirse cambios, estos serán debidamente notificados.

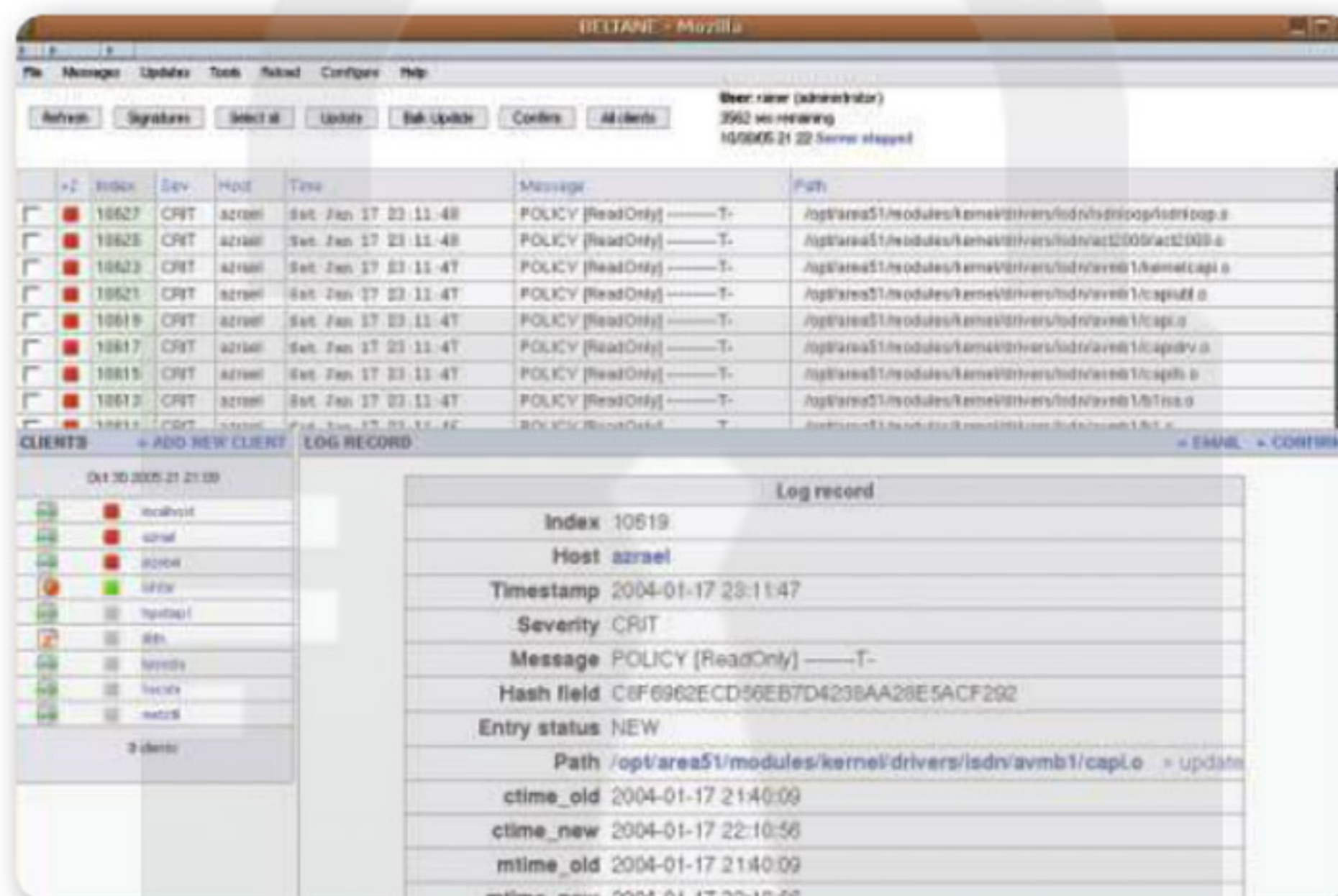


Figura 31. Samhain es uno de los mejores HIDS de código abierto disponibles para sistemas UNIX.

Cada herramienta particular puede tener características adicionales, pero todas, básicamente, apuntan a detectar comportamientos extraños o no deseados en el sistema operativo, y a reportarlos y/o bloquearlos.

Honeypots

Este tipo de sistemas busca implementar una especie de **trampa**, para atraer tanto a los atacantes como al malware que intente dispersarse automáticamente. La idea principal se basa en el concepto de que, si el sistema se encuentra exclusivamente dedicado a su función de honeypot, cualquier intento de conexión que se haga sobre él puede considerarse como **malintencionada**, porque ese dispositivo no cumple ninguna función real para la organización.



Figura 32. ProjectHoneypot permite que cada dueño de un dominio pueda contribuir a detectar spammers.

Los honeypots suelen emular distintos sistemas operativos –Microsoft Windows, GNU/Linux, Cisco IOS, etcétera–, y aparentar el ofrecimiento de servicios vulnerables (como software desactualizado o mal configurado), para atraer, en particular, a los atacantes que realizan escaneos de la red. Verdaderamente, ninguno de estos servicios es prestado, sino que se utilizan programas falsos que escuchan en los puertos correspondientes, y responden de manera igual o similar a los sistemas originales. De esta manera, los atacantes nunca tomarían control real del sistema honeypot.



HONEYPOTS ESPECÍFICOS

Existen honeypots desarrollados para emular exclusivamente un tipo particular de sistema, con el objetivo de atraer solo cierta clase de ataques o malware. Dos ejemplos son **Artemisa** (<http://artemisa.sourceforge.net>), que emula un sistema de voz sobre IP; y **SpamHole**, que emula un servidor de correo mal configurado (<http://sourceforge.net/projects/spamhole>).

Además, suelen utilizarse técnicas para tomar automáticamente direcciones de red libres, y contestar a conexiones de red realizadas a direcciones que no están ocupadas por ningún sistema real.

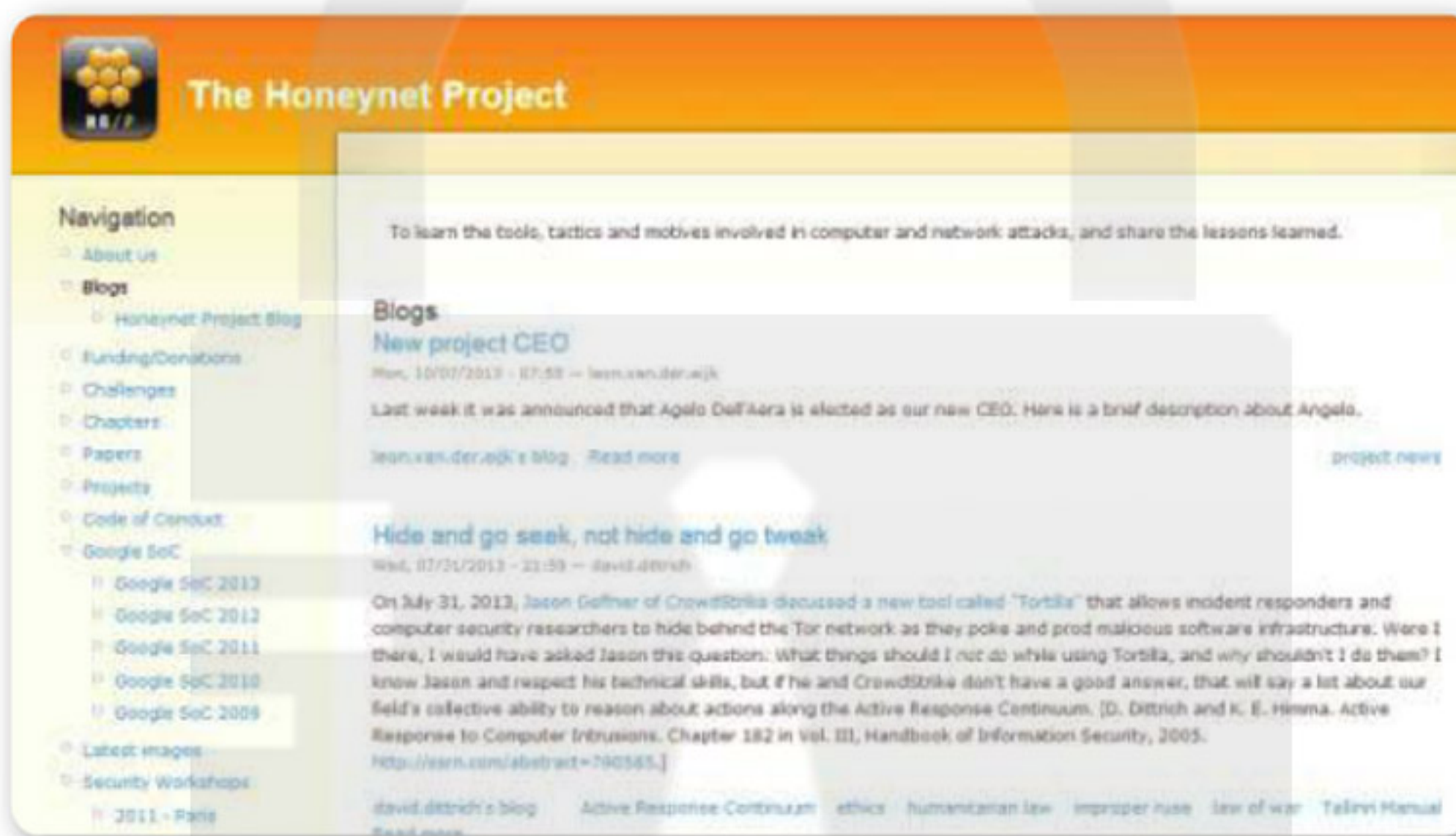


Figura 33. HoneyNet (www.honeynet.org) investiga los últimos ataques y desarrolla herramientas de código abierto para aumentar la seguridad de los sistemas.

Obviamente, la implementación de este tipo de sistemas requiere analizar constantemente toda conexión que se realiza a ellos. Ya sea de forma automática (recomendada) o manual, debemos estar al tanto de los sistemas que envían tráfico a las direcciones de red tomadas por nuestro honeypot.



Gestión de parches

Una de las tareas más importantes y críticas en cuanto a la administración de sistemas operativos es la gestión de los parches, que comprende tanto la selección, como la manera y el momento de aplicarlos. Este tipo de decisiones debe tomarse sobre la base de varios factores, como el propósito del sistema, su criticidad y las características del parche en cuestión.

Como analizamos en capítulos anteriores, es de gran utilidad contar con sistemas dedicados exclusivamente a pruebas, para evitar el hecho de aplicar un parche sin saber qué impacto puede tener en el funcionamiento de nuestro sistema de producción.

Cada sistema operativo cuenta con sus herramientas propias para realizar la gestión de parches y actualizaciones. En el caso de Microsoft, disponemos de la plataforma WSUS (*Windows Server Update Services*), que es de uso gratuito y nos ofrece una gran cantidad de funciones, tendientes a satisfacer las necesidades de la mayoría de las empresas.

En lo que se refiere a plataformas UNIX, cada distribución incluye sus herramientas particulares. Y siempre tenemos la opción de personalizar el comportamiento a través de scripts.



RESUMEN



En este capítulo pudimos analizar las características de los sistemas operativos pertenecientes a la familia Microsoft y Unix, conocimos sus diferencias y entregamos diversos consejos para aumentar su nivel de seguridad. Revisamos el proceso de hardening y detallamos el funcionamiento de Network Access Control; más adelante revisamos el concepto de malware y detallamos la forma correcta de aprovechar un firewall y un sistema de backups. Analizamos la autenticación multifactor y vimos cómo funcionan los servidores de autenticación. También revisamos cómo podemos efectuar un completo análisis de logs y conocimos algunas aplicaciones para detectar intrusos. Para terminar, aprendimos cómo gestionar parches para el sistema operativo.

Actividades

TEST DE AUTOEVALUACIÓN

- 1 ¿Qué aspectos debemos tener en cuenta al elegir un sistema operativo?
- 2 ¿Qué es y por qué es importante el hardening de sistemas?
- 3 ¿Para qué sirve la autenticación multifactor?
- 4 ¿En qué casos puede ser beneficioso implementar port knocking?
- 5 ¿Qué es y para qué sirve un honeypot?



PROFESOR EN LÍNEA



Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: **profesor@redusers.com**

Tendencias actuales

En este capítulo nos dedicaremos a reconocer los peligros de las tecnologías móviles, revisaremos las consideraciones adecuadas para implementar tecnologías de virtualización, y obtendremos una completa visión acerca de las nuevas tendencias en tecnología y lo que implican para la seguridad.

▼ Tecnología	2	▼ Tecnología móvil	27
▼ Web 2.0.....	2	▼ Ataques dirigidos	30
▼ Servicios de mensajería	9	▼ Expectativas para el futuro	34
▼ VoIP.....	14	▼ Resumen.....	35
▼ Virtualización	17	▼ Actividades.....	36
▼ Cloud computing.....	23		



Tecnología

Como ya hemos analizado durante los capítulos anteriores, la tecnología avanza constantemente, evoluciona a un ritmo acelerado. Por desgracia, los peligros que podemos encontrar avanzan de la misma forma.

Podemos afirmar, sin temor a equivocarnos, que hace muchos años que no tenemos **tranquilidad** en el ambiente tecnológico. Es decir, prácticamente todos los años aparece un nuevo producto o tecnología que genera una revolución en nuestras vidas. Esto provoca cambios en la forma de trabajar, de pensar y de vivir, por lo que, a veces, la tecnología marca las tendencias, y a veces, tiene que evolucionar para seguirse el paso a sí misma. Particularmente, la seguridad informática se encuentra siempre un paso por detrás del resto de los aspectos tecnológicos, no por carecer de creatividad o de especialistas, sino porque su propósito es reaccionar ante cualquier nuevo comportamiento que pudiera poner en peligro tanto a las personas como a las organizaciones que utilizan las nuevas tecnologías.

Nuestra misión es que las personas y las organizaciones puedan aprovechar al máximo las nuevas tecnologías, teniendo cuidado de que se las utilice en forma segura.

Esto hace que la profesión sea extremadamente emocionante, y le da una naturaleza de investigación constante, que pocas otras profesiones encuentran. En las páginas siguientes analizaremos cuáles son las tecnologías con las cuales convivimos a diario y cómo podemos implementarlas sin poner en riesgo la seguridad de la organización.



Web 2.0

Este concepto no se refiere a una actualización de las tecnologías o protocolos, ni a un uso puntual de ellos, sino más bien a una nueva forma de desarrollo que tiene como objetivo poner a la Web en el centro de la escena para facilitar la posibilidad de compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración. Esto dio nacimiento a las



comunidades web, los servicios web, las aplicaciones web, las **redes sociales**, los **servicios de alojamiento de videos**, las **wikis**, los **blogs**, y otros servicios.

Particularmente, algunas de las tecnologías más involucradas en la **Web 2.0** son **CSS**, **AJAX**, **RSS/ATOM**, **XML** y **JSON**, entre otras. En esta Web, el usuario es el protagonista principal, que tiene la capacidad de publicar contenidos, conectarse con otras personas e interactuar con toda la infraestructura disponible, que antes se utilizaba solo para leer información.

Si bien el concepto de **Web 3.0** (principalmente, la Web semántica) está rondando la escena hace varios años, podemos decir que el gran salto de paradigma fue dado por lo que sería su predecesor, en el cual encontramos una fuerte cantidad de nuevos beneficios y peligros.

LAS TECNOLOGÍAS
DE LA WEB 2.0 SON
CSS, AJAX, RSS/
ATOM, XML Y JSON,
ENTRE OTRAS



Redes sociales

Sin lugar a dudas, las redes sociales, como **Facebook**, **Twitter** y **GooglePlus**, son la nueva tecnología en expansión. Su misión: permitir que cualquier usuario genere contactos con otras personas y comparta información rápidamente, aunque también permiten la proliferación de malware, ataques y estafas.

Para una organización, antes era fácil bloquear los accesos a estos tipos de redes, que solamente se utilizaban para el ocio. En la actualidad, existen redes desarrolladas con fines laborales, como **LinkedIn**, que las mismas organizaciones emplean para reclutar personal o hacer otros contactos de negocios. También Facebook se utiliza como medio de promoción para las empresas. Por estos motivos, ya es casi imposible bloquear este tipo de accesos, porque la publicidad web se encuentra dentro de los planes de toda organización actual. Pero debemos ser cuidadosos, y permitir el acceso a este tipo de redes solo a aquellas personas que verdaderamente lo necesitan.



Figura 1. Facebook se ha convertido en la red social más popular, por lo que se ha vuelto el objetivo de muchísimos ataques. Para obtener más información acerca de buenas prácticas de seguridad en su uso, podemos visitar **www.facebook.com/safety**.

Otra problemática que se genera en todas las organizaciones es que los usuarios pueden revelar información confidencial de la empresa a través de estas redes, aun cuando no están en la oficina, sino en sus casas usando sus computadoras personales. Por lo tanto, es de vital importancia contar con un buen plan de capacitación, que haga entender a los usuarios los peligros potenciales a los que exponen a su organización al divulgar información privada.

Google hacking

Con este término se conoce a las técnicas para recabar información de una organización a través de los buscadores de internet –particularmente, utilizando **Google**. Esto no es algo que pueda catalogarse como un ataque en sí, pero sí puede ser de gran importancia para determinar el éxito o el fracaso de un atacante.

Los buscadores de internet almacenan muchísima información (quizá, demasiada) acerca de los sitios web que analizan. Además, buscadores como Google ofrecen varias opciones de búsqueda para encontrar tipos de archivo específicos, buscar solo dentro de un dominio particular, y muchos otros parámetros.

Para protegernos de las búsquedas de información sensible en nuestros servidores web, podemos enumerar las siguientes consideraciones:

- No alojar información verdaderamente confidencial en los servidores web.
- Prohibir el listado de directorios.
- Utilizar el archivo **robots.TXT** para definir qué secciones de nuestro sitio web van a catalogar los robots de los buscadores.
- Proteger las secciones privadas de nuestro sitio web mediante contraseñas.

Si queremos que nuestro sitio web detalle qué partes no deben ser analizadas por los robots de los buscadores, podemos ubicar el archivo **robots.txt** en la raíz, con un contenido como el siguiente:

```
User-agent: *  
Disallow: /administrator/  
Disallow: /images/  
Disallow: /includes/  
Disallow: /templates/  
Disallow: /tmp/
```

Pero debemos recordar que este tipo de configuraciones solo funciona si los robots respetan estos archivos. Los buscadores más famosos, como **Google**, **Yahoo!** y **Bing**, sí lo hacen.

Como siempre, uno de los métodos más efectivos para protegernos, es verificar qué información relacionada con nuestra organización aparece en

los buscadores web. Para esto, la forma más sencilla es ingresar en el sitio de algunos buscadores y realizar consultas a partir del nombre de nuestra empresa y de otros aspectos relacionados con ella, como teléfonos, direcciones de correo electrónico, etcétera.

Phishing y robo de identidad

Este concepto no es nuevo, pero ha evolucionado a la par de las nuevas tecnologías. Se trata, básicamente, de estafas que se realizan a partir de generar una falsa identidad, para que el usuario crea que está ante un ente de su confianza y, así, entregue información confidencial, como credenciales, números de cuentas bancarias, datos personales, y más.

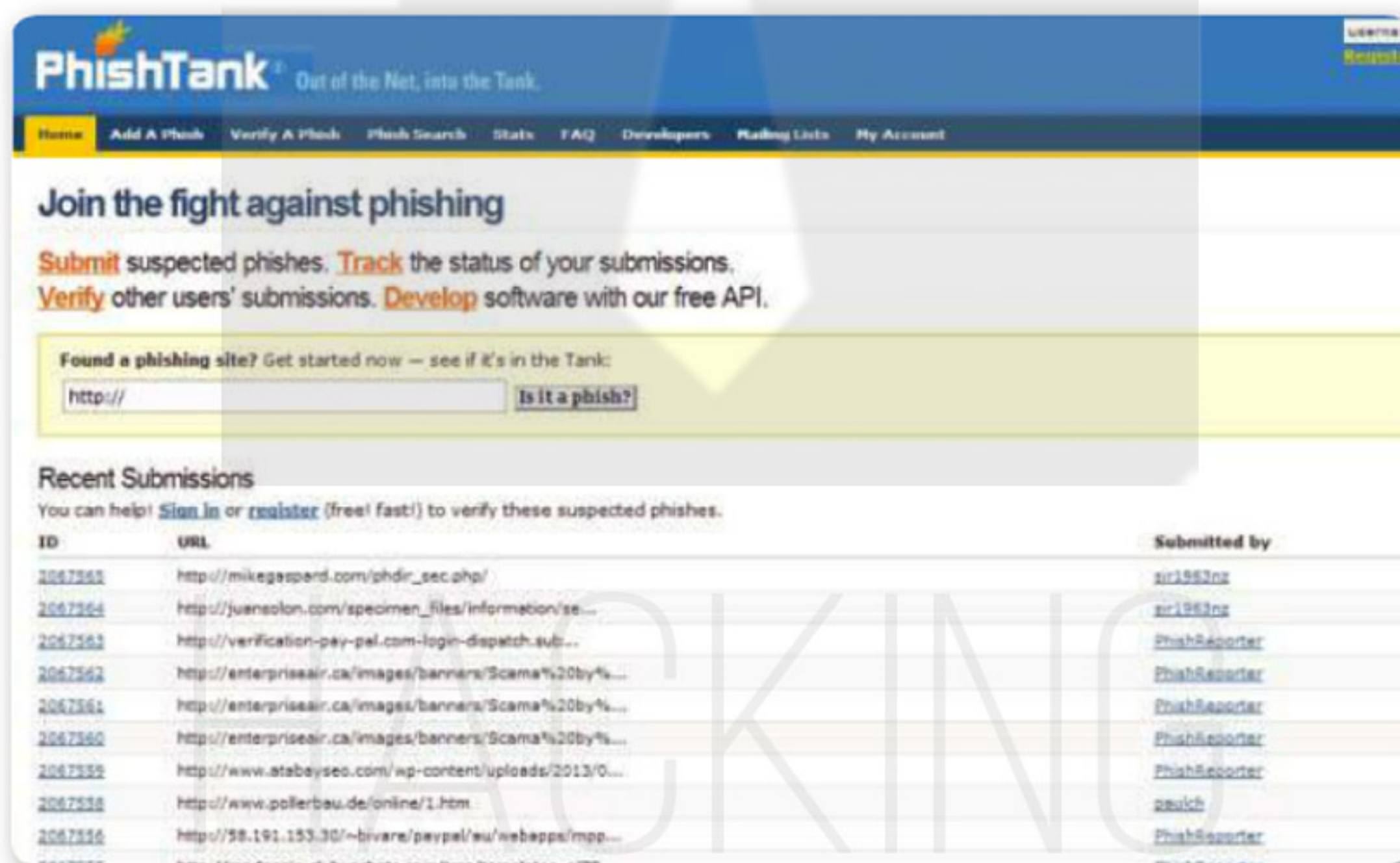


Figura 2. En el sitio web www.phishtank.com encontramos información importante acerca de los ataques de phishing.

Si bien podemos encontrar que existen muchas tecnologías y técnicas involucradas (como el *pharming*) en los actos de phishing, todas pasan a través de la interacción del usuario, para que, de un modo u otro, confíe

en el que, en realidad, es un atacante. Como podemos notar, esto no es más que una estafa electrónica.



Figura 3. El **Anti-Phishing Working Group** es un consorcio internacional que reúne a varias organizaciones ocupadas en la lucha contra el phishing (www.antiphishing.org).

Con respecto al robo de identidad, este suele realizarse una vez completado un ataque de phishing, aunque también existen otras formas de



DOMINIO PÚBLICO

Es de suma importancia que los usuarios tomen conciencia y entiendan que todo lo que se publica en los medios de internet se vuelve automáticamente de dominio público. Más allá de que hayamos configurado opciones de privacidad en las redes sociales, actualmente, en internet, el concepto de privacidad no existe.

acceder a los datos necesarios para hacerlo. El objetivo principal aquí es suplantar la identidad de una persona para realizar compras o pagos a su nombre. Este tipo de ataques es el de más alto crecimiento, y representa un gran riesgo para todas las personas. No está relacionado directamente con la seguridad organizacional, sino más bien con la seguridad personal. Estos son algunos consejos para evitar ser víctimas del phishing:

- Escribir (no hacer clic en los enlaces) las direcciones de sitios web importantes, como entidades bancarias u otros sitios que nos soliciten información confidencial.
- Cerrar las sesiones de los sitios web y las aplicaciones confidenciales.
- Tener en cuenta que los **bancos** y otras entidades nunca nos solicitarán que les enviemos nuestras claves de acceso ni ningún otro tipo de dato confidencial.
- Jamás utilizar máquinas de **acceso público**, como las de **cibercafés**, para enviar o recibir información confidencial.



Figura 4. En el sitio web de **Identidad Robada** podemos encontrar mucha información acerca de los robos de identidad (www.identidadrobada.com).

Estos consejos, entre otros, son los que debemos comunicar a los integrantes de nuestra organización para que estén al tanto acerca de cómo evitar ser víctimas de este tipo de ataques.



Servicios de mensajería

Podemos definir los servicios de mensajería como **servicios que permiten intercambiar mensajes entre usuarios**. Estos servicios se han vuelto muy populares en internet, porque son, básicamente, la gran herramienta de comunicación entre usuarios. A medida que estos servicios fueron evolucionando, se los ha dotado de más características que potencian la cantidad de contenidos que se pueden transmitir. Recordemos que, en un principio, solamente existían mensajes en texto plano, a través del correo electrónico o el IRC. En la actualidad, contamos con varias herramientas de mensajería, de las cuales haremos un análisis de seguridad.

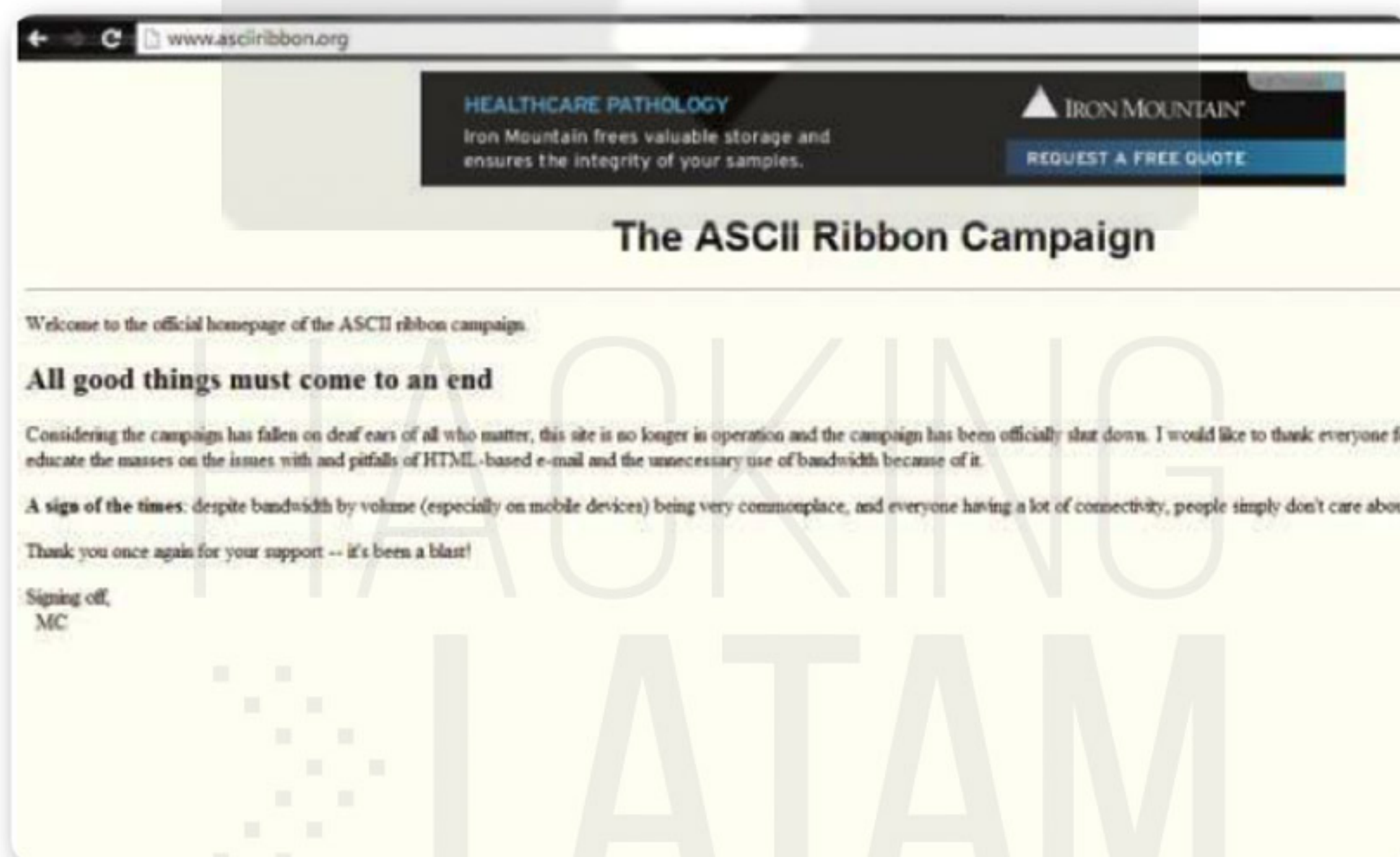


Figura 5. El proyecto **ASCII Ribbon**, ahora discontinuado, buscó generar conciencia sobre las ventajas del correo electrónico en texto plano.

Mensajería instantánea

Los servicios de mensajería instantánea son unos de los más utilizados por los internautas, tanto en sus hogares como en las oficinas. Estos han pasado de ser un simple **IRC (chat simple)**, a convertirse en herramientas y protocolos más avanzados, como **Skype**, entre otros. Con esta evolución, ha surgido una gran cantidad de problemas de seguridad, que debemos tener en cuenta. Si a esto le sumamos que, actualmente, muchos sitios web cuentan con mensajería en línea, como el mensajero de Facebook, podemos observar que las posibilidades que tiene un usuario para intercambiar mensajes con otro son prácticamente ilimitadas, por lo que se vuelve una tarea muy compleja, y hasta agotadora, intentar bloquear todos estos protocolos y herramientas.

Si necesitamos hacerlo, podemos simplificar el trabajo a través de algunos dispositivos **UTM**, como los desarrollados por **Fortinet**, **Watchguard** o **Checkpoint**, entre otros, que cuentan con grandes capacidades de filtrado por protocolo y aplicación.

Transferencia de archivos

Uno de los grandes cambios de los servicios de mensajería ha sido la capacidad para enviar y recibir archivos. Esto ha dotado a los usuarios de una tremenda facilidad para transferir contenidos de manera instantánea, pero también es una gran posibilidad para los atacantes de mandar todo tipo de malware.

Es por eso que muchas veces se critica el uso de los servicios de mensajería por los **riesgos de seguridad implicados**. El problema es que, de una forma u otra, la transferencia de archivos debe ser permitida en una organización. Y siempre es mejor que lo hagamos de manera transparente y amigable para el usuario, en vez de forzarlo a buscar métodos no autorizados para transferir archivos, que podrían poner en peligro a nuestra empresa.

Algunas de las opciones de código abierto que tenemos para bloquear la mensajería instantánea son el firewall gratuito **Untangle** (www.untangle.com), o la combinación de algunos productos, como el

proxy Squid (www.squid-cache.org) y alguna otra herramienta de filtrado de paquetes, como **IPTables** para sistemas **Linux**.

Los mismos dispositivos de firewall nombrados en el apartado anterior tienen la capacidad de realizar análisis antimalware, bloqueo de transferencias por tipo de archivo y algunos otros filtros que pueden sernos de utilidad.

Fuga de información

Una de las grandes preocupaciones actuales de las organizaciones con respecto a la seguridad es la **fuga de información confidencial**. Esta situación se ve agravada por la gran cantidad de medios de comunicación con los que contamos al tener una conexión a internet.

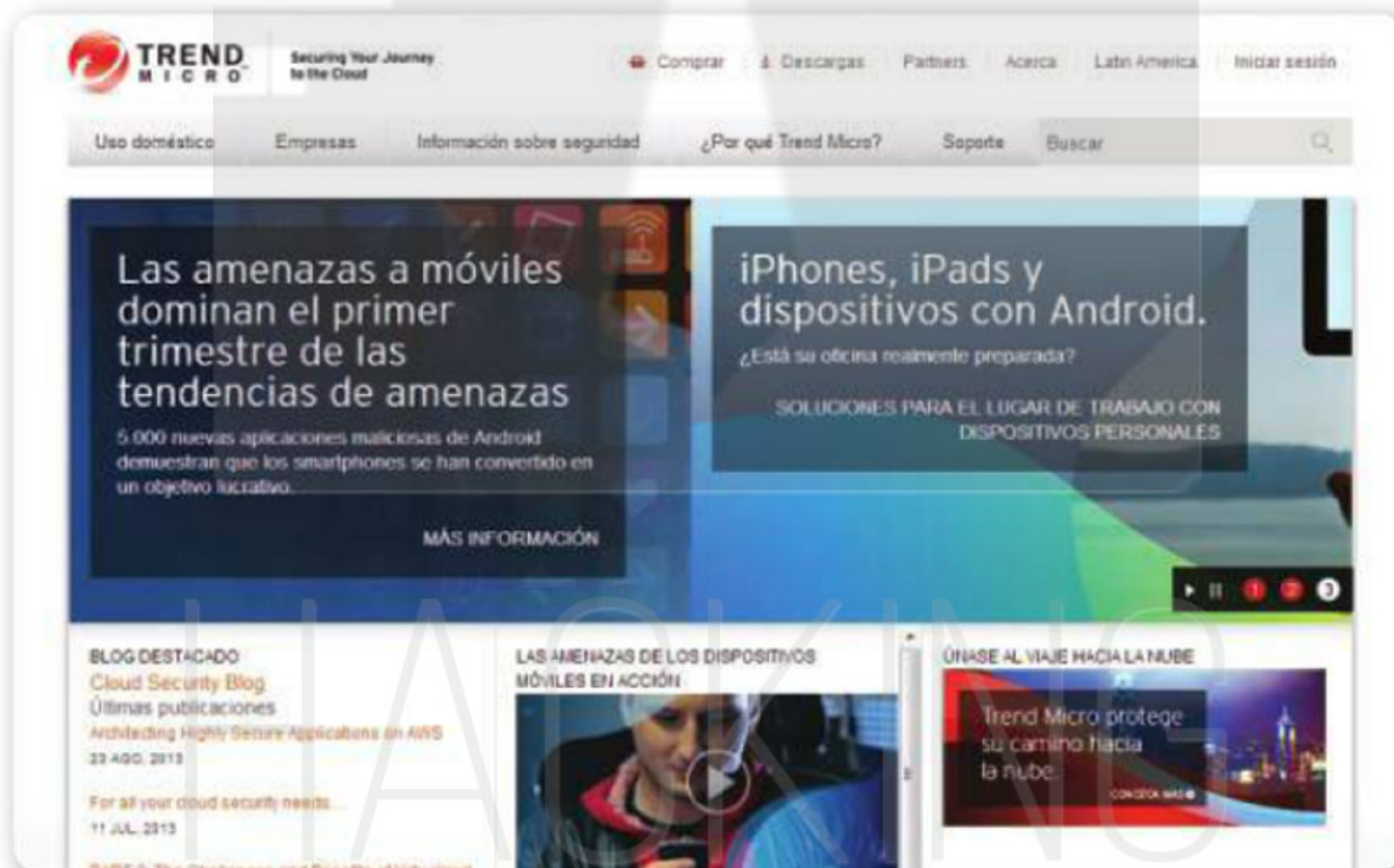


Figura 6. Varios fabricantes de software de seguridad, como **TrendMicro**, ofrecen productos para evitar la fuga de información y la pérdida de datos (www.trendmicro.com).

La fuga de información debe encararse desde varios frentes para poder combatirla adecuadamente. No estamos hablando de un dispositivo, pro-

toloco o herramienta en particular, sino que debemos proteger una infinidad de métodos para transferir información.

Es por eso que, por sobre todas las cosas, los usuarios deben estar al tanto de qué información pueden compartir abiertamente y cuál deben mantener privada. Por lo tanto, podemos observar que la primera medida para luchar contra la fuga de información es la capacitación de los usuarios.



Figura 7. El proyecto de código abierto **MyDLP** desarrolla un software destinado a la protección contra la fuga y la pérdida de datos. En la imagen podemos observar su uso para filtrar ciertos tipos de datos, como números de tarjetas de crédito (www.mydlp.org).

Comunicaciones no deseadas (spam)

Los **mensajes no deseados (spam)** han dejado de pertenecer solamente a los servicios de correo electrónico, y ahora forman parte de cualquier servicio de mensajería, aunque el correo se lleva la mayor parte de este tipo de transferencia.



Figura 8. El proyecto de código abierto **SpamAssassin** es el más reconocido filtro antispam. Es desarrollado por la fundación **Apache** y cuenta con una gran capacidad de filtrado, además de tener una amplia documentación.

En una organización, el bloqueo de spam es estrictamente necesario, porque este alcanza niveles tan altos, que reduce de manera notable las capacidades de trabajo de los empleados. Si estos reciben enormes cantidades de mensajes no deseados, se pierde mucho tiempo en catalogar a mano qué es spam y qué no lo es.



TÉCNICAS ANTISPAM



En el sitio web Wikipedia (http://en.wikipedia.org/wiki/Anti-spam_techniques) podemos encontrar un excelente artículo que detalla varias de las técnicas antispam más efectivas, tanto para los usuarios finales como para los administradores de servicios de correo electrónico. Esta enciclopedia libre es un recurso de gran valor para todas nuestras tareas de investigación.



Figura 9. El sitio web **Spamhaus** mantiene varias **listas negras** con dominios y direcciones IP que son frecuentemente utilizados para enviar spam (www.spamhaus.org).

VoIP

Los **servicios de voz sobre IP (VoIP)** se han vuelto extremadamente populares, al ofrecer mejores características y menor costo que la telefonía tradicional. Es por eso que su uso crece año a año, y las organizaciones implementan este tipo de soluciones para reemplazar las viejas tecnologías y unificar sus redes de comunicación.

Como toda tecnología, los protocolos relacionados con VoIP presentan ciertas falencias de seguridad, sobre todo, si están mal configurados. Esto podría permitir tanto la escucha de conversaciones como la realización de llamadas por parte de terceros, que obligan a la organización a pagar por comunicaciones que no realizó.

Es por eso que, en caso de implementar VoIP en nuestra organización, debemos tomar los recaudos necesarios, y analizar tanto los protocolos

que vamos a utilizar, como las herramientas y productos por implementar. Algunos consejos de seguridad para los servicios VoIP son: encriptar las comunicaciones, revisar la seguridad de los protocolos TCP/IP que dan soporte a estos servicios y monitorear el uso de las centrales de telefonía IP.

La combinación de los protocolos más utilizada en los ambientes VoIP son **SIP** (*Session Initiation Protocol*) para el inicio y la terminación de llamadas, y **RTP** (*Real-time Transport Protocol*) para el transporte del audio. Es muy aconsejable emplear alguna variante encriptada de ellos, como **SRTP**, que, básicamente, es lo mismo que RTP pero con **encriptación de tráfico**.



Figura 10. En el sitio web **VoIP-Info** podemos encontrar una gran cantidad de información acerca de productos, protocolos y herramientas relacionadas con la tecnología VoIP, y también recomendaciones de seguridad (www.voip-info.org).

Espionaje de comunicaciones

Los medios físicos que transportan las comunicaciones tradicionales suelen ser, por naturaleza, muy difíciles de interceptar para capturar la información que viaja a través de ellos, debido a que esto suele producir

EN LAS COMUNICACIONES IP SE VUELVE FÁCIL CAPTURAR INFORMACIÓN



cortes u otras anomalías en la comunicación, que son rápidamente detectables. Además, se requiere acceso físico a algún punto del medio de transporte para efectuar alguna captura.

Sin embargo, en el caso de las comunicaciones IP, se vuelve muchísimo más fácil capturar información de manera remota, y es posible hacerlo sin que esto produzca un impacto negativo o extraño en la comunicación. Existen varios programas desarrollados exclusivamente para capturar paquetes con audio, para luego ensam-

blarlos y obtener una copia exacta de toda la comunicación realizada.

Es por eso que resulta de suma importancia la encriptación del tráfico que contenga comunicaciones críticas o privadas. Para esto, podemos utilizar protocolos como **SRTP**, **IPSec** o algún otro tipo de enlaces del tipo **VPN**.

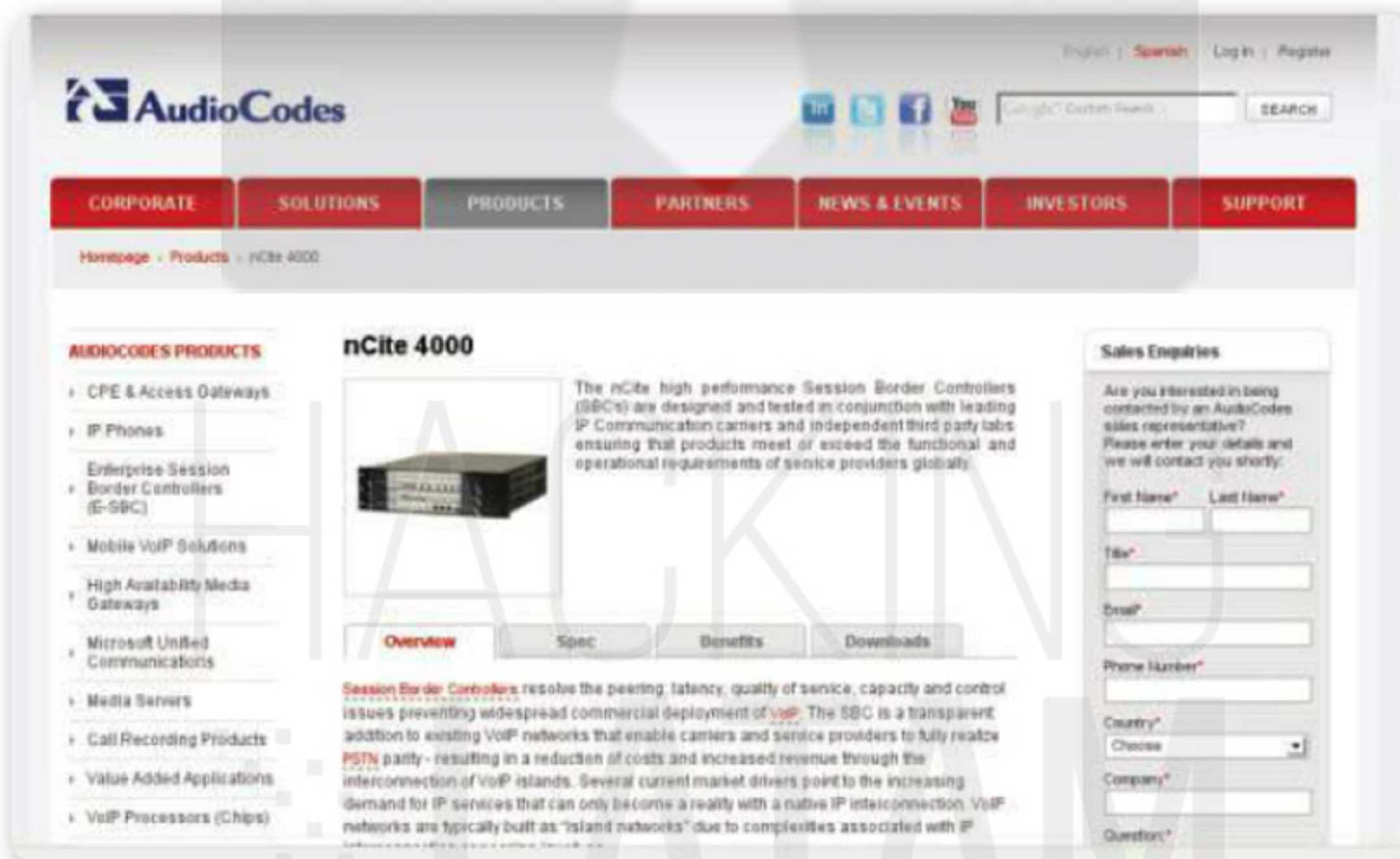


Figura 11. El **nCite 4000**, de **Audiocodes**, es un equipo que, entre otras cosas, provee seguridad para las comunicaciones **VoIP**, con capacidades de encriptación, protección contra ataques **DoS**, validación de protocolos y muchas otras funciones.

Videoconferencias

Con la capacidad de transportar datos de audio sobre redes IP para realizar llamadas telefónicas, el salto a las videoconferencias (llamadas con video incluido) fue sencillo, porque solo se incluye un nuevo tipo de datos, utilizando la misma arquitectura VoIP. La gran diferencia que se presenta con VoIP es que este tipo de llamadas no puede ser transmitida a través de la red de telefonía tradicional (porque esta no cuenta con soporte de video).

Sin entrar en más detalles, podemos decir que todas las medidas de seguridad requeridas para VoIP se aplican a las llamadas de videoconferencia, y que debemos encriptar y asegurar los datos que transmitimos.



Virtualización

El uso de este tipo de tecnologías ha crecido enormemente en los últimos años, a tal punto que podemos afirmar que la mayoría de las organizaciones las implementa de uno u otro modo. La reducción de costos y las mejoras en los procesos de gestión que nos brinda la virtualización son evidentes, y hacen que cualquier empresa cuente con este tipo de proyectos dentro de sus planes. Nosotros debemos estar preparados para responder a las cuestiones de seguridad relacionadas con estas tecnologías.

En la actualidad, existen varios fabricantes de **plataformas de virtualización**, cada uno con sus ventajas y desventajas. La decisión de utilizar una u otra tecnología debe tomarse sobre la base de las necesidades de cada organización.

También debemos considerar hacer una inversión en herramientas que nos faciliten la gestión de la infraestructura –copias de respaldo, recuperación en caliente, balanceo de cargas, etcétera.

A continuación, definimos algunos de los puntos más importantes para tener en cuenta con respecto a la seguridad cuando nos enfrentamos a las infraestructuras virtuales.

Asegurar correctamente los equipos de host

Los equipos que contienen las **máquinas virtuales** deben estar adecuadamente asegurados, debido a que una falla podría comprometer la confidencialidad, integridad o disponibilidad de todas las máquinas virtuales alojadas en ellos. También debemos recordar que los equipos host cuentan con un sistema operativo que puede ser atacado, por lo que debemos verificar con detenimiento la documentación del fabricante, a fin de configurar toda la solución como corresponde.

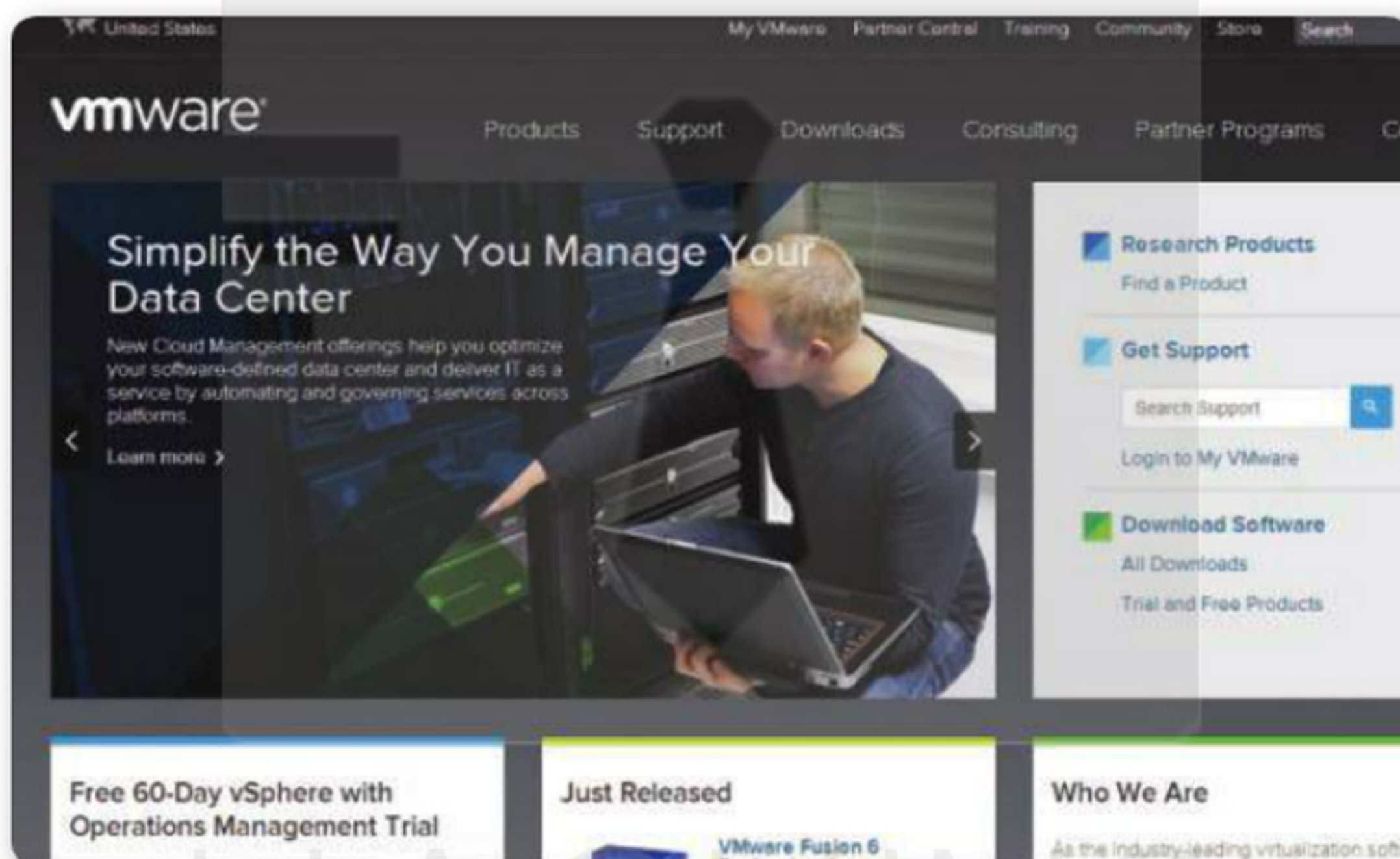


Figura 12. VMWare es el líder en soluciones de virtualización. Cuenta con una gran cantidad de productos, y varios de ellos, con funciones de seguridad avanzadas (www.vmware.com).

Asegurar los medios de almacenamiento

En las soluciones de virtualización medianas o grandes se recomienda utilizar dispositivos de almacenamiento –conocidos como *storage*– dedicados para aumentar la capacidad, la **velocidad de lectura/escritura** y las posibilidades para gestionar la información. Si implementamos este tipo

de soluciones, debemos considerar a nuestros **equipos de storage** como críticos, porque podrían exponernos a una destrucción de los datos o a la fuga de información. Recordemos que en los ambientes virtuales, cada máquina virtual está formada por algunos pocos archivos. Si estos se ven comprometidos, un atacante podría llevarse una copia completa del sistema o destruir nuestros sistemas productivos.

Asegurar cada una de las máquinas virtuales

Cada máquina virtual debe ser asegurada tal y como se lo haría en caso de que fuera una máquina física. Es importante tener esto en cuenta, porque la facilidad de crear, copiar y eliminar máquinas virtuales muchas veces genera una falsa sensación de sencillez, que lleva a algunos administradores a olvidar los procesos de seguridad.

Utilizar adecuadamente las plantillas de máquinas virtuales

Para simplificar las tareas expuestas en el punto anterior, es una buena práctica de seguridad definir una plantilla de sistema que ya cuente con todas las configuraciones necesarias, para así poder crear fácil y rápidamente otros sistemas a partir de ella. Es de suma importancia que esta



MÁQUINAS VIRTUALES



Uno de los inconvenientes más importantes de las máquinas virtuales es que agregan complejidad al sistema en tiempo de ejecución. Esto representa una ralentización del sistema; el programa no alcanzará la misma velocidad de ejecución que si se instalase directamente en el sistema operativo anfitrión o host.

plantilla esté correctamente configurada, dado que un error en ella provocaría fallas en todos los servidores creados.



Figura 13. El fabricante de productos de seguridad **McAfee** cuenta con varias soluciones desarrolladas para aumentar la seguridad en entornos virtualizados (www.mcafee.com).

Controlar adecuadamente la gestión de la infraestructura virtual

La facilidad de administración que presentan las infraestructuras virtuales muchas veces hace que cualquier persona del sector de IT cree, modifique o elimine máquinas virtuales. Esto es un gran riesgo no solo para la seguridad, sino también para el rendimiento de las máquinas virtuales. Debemos recordar que, en ambientes de producción, la creación o modificación de las configuraciones podría llevar a un consumo excesivo de recursos de hardware o a fallas inesperadas si se modifica el hardware virtual sin tener en cuenta las configuraciones necesarias para el sistema operativo que corre sobre él.

Implementar filtros físicos en las zonas de alta criticidad

Aun cuando los fabricantes de soluciones de virtualización prometen que sus productos brindan igual o mayor seguridad que las separaciones físicas, debemos considerar separar los equipos que contienen máquinas virtuales de prueba, de los que contienen máquinas virtuales críticas para la operatoria de nuestra organización. Recordemos que los ambientes de pruebas suelen ser más propensos a errores o malas configuraciones, de modo que no debemos permitir que estas fallas dejen expuesta la infraestructura de producción. En caso de que no sea posible realizar separaciones físicas, deberemos asegurarnos de aprovechar todas las características de seguridad con las que cuente la solución que estamos implementando.

Los sistemas host son tan críticos como la máquina virtual que corre sobre ellos

Es preciso recordar esto al configurar los sistemas host. Si es que vamos a alojar dentro de ellos máquinas virtuales que tengan una alta criticidad para la organización, debemos catalogar estos sistemas host con la misma criticidad que las máquinas virtuales que contienen. Como analizamos anteriormente, una falla en los sistemas host podría comprometer las máquinas virtuales que albergan.

Separar una red para administración, de la infraestructura virtual

Las telecomunicaciones que corresponden a la administración, tanto de los sistemas host como de las máquinas virtuales que contienen, deben estar separadas del resto del tráfico de la red, a fin de garantizar que siempre podremos administrar de manera adecuada la infraestructura. Recordemos que una red plana, sin segmentar, podría colapsar si cualquiera de sus componentes sufriera fallas de algún tipo. Es por eso que debemos prevenir el hecho de quedarnos sin la capacidad de gestionar la infraes-

estructura. Esto puede lograrse implementando separaciones tanto físicas –hardware distinto– como lógicas –distintas redes virtuales, o VLANs.

Garantizar la conectividad de la infraestructura con las demás redes

Muchas veces se hace hincapié en garantizar la disponibilidad de las máquinas virtuales, implementando redundancia, tanto de software como de hardware. Y esto está muy bien, pero también debemos considerar el caso de que el hardware de telecomunicaciones presente fallas. La pérdida de conectividad entre la infraestructura virtual y el resto de la red podría significar una pérdida total de disponibilidad de los servicios. Es por eso que precisamos garantizar el funcionamiento de la red, de ser posible, utilizando hardware redundante.

Implementar separación de tareas para la gestión de la infraestructura

Es ampliamente recomendable que por lo menos dos personas estén encargadas de gestionar la infraestructura virtual, utilizando lo que se conoce como **separación de roles**, para que ninguna desarrolle completamente las tareas de gestión. Esto disminuye de manera notable la probabilidad de errores, al requerir que al menos dos personas estén de acuerdo con los cambios que habrá que realizar.



EMULACIÓN DE HARDWARE



El sistema pionero que utilizó la emulación de hardware fue la **CP-40**, la primera versión (1967) de la **CP/CMS** de IBM (1967-1972) y el precursor de la familia **VM** de IBM. Consideremos que con la arquitectura VM, la mayor parte de usuarios controlan un sistema operativo monousuario simple llamado **CMS**, el cual se ejecuta en la máquina virtual VM.



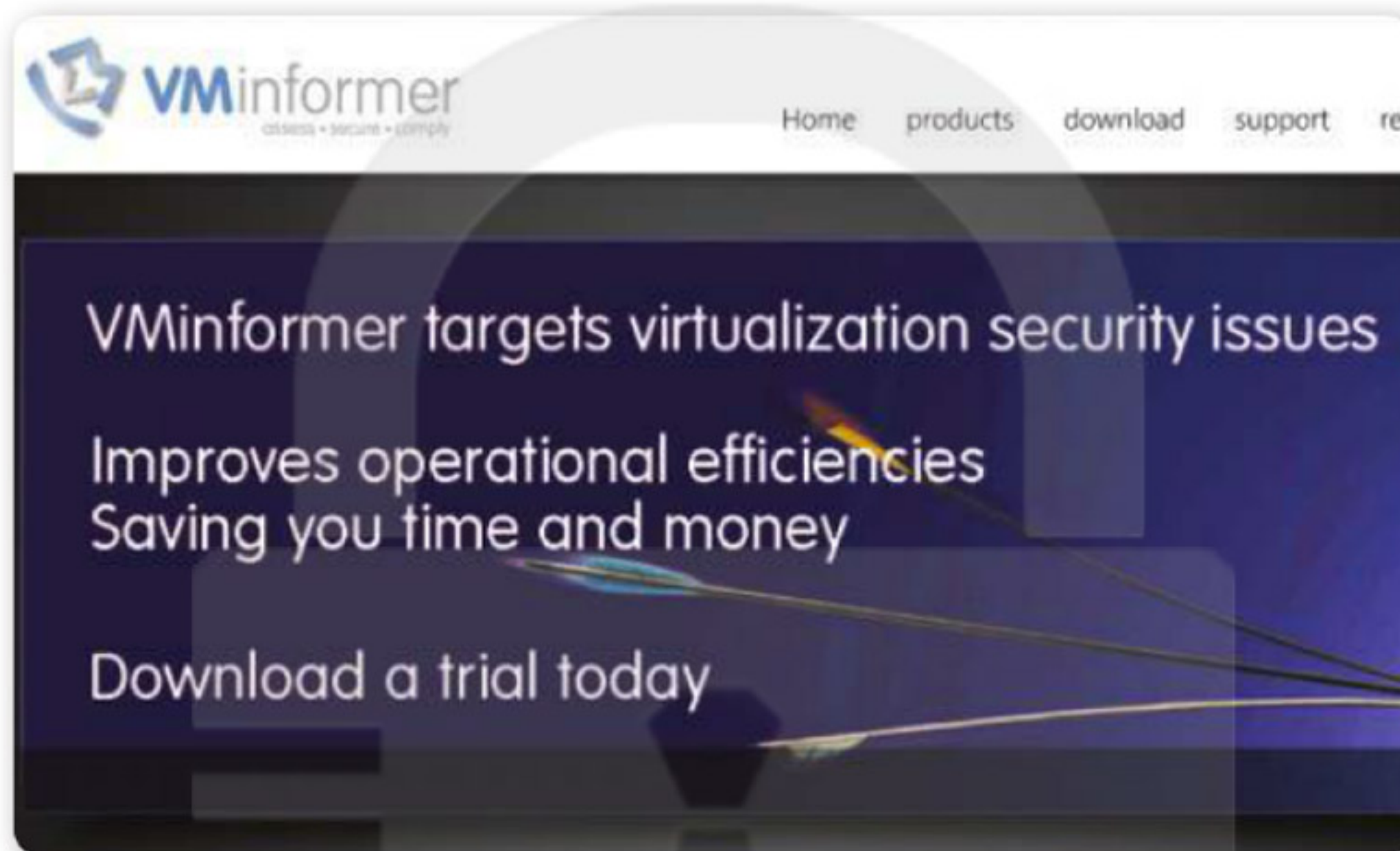


Figura 14. Existen varios fabricantes, como **VMinformer**, que se dedican pura y exclusivamente a desarrollar soluciones de seguridad y auditoría para ambientes virtualizados (www.vminformer.com).

Contar con redundancia de equipos

Como la falla de un sistema host implica la falla de todas las máquinas virtuales que corren sobre él, es ampliamente recomendable que implementemos redundancia de hardware o soluciones de virtualización que nos permitan contar con varios sistemas host distintos, que tengan la capacidad de suplantarse entre sí en caso de que alguno presente un problema.



Cloud computing

Una de las tecnologías actuales, que nació de la mano de la virtualización, es la computación en la nube o *cloud computing*, que nos permite brindar y utilizar servicios alojados en internet. Si bien esto permite tener una gran reducción de costos y nuevas capacidades para brindar servicios, también es muy cuestionado desde el punto de vista de la seguridad, debido a que los

equipos en los que las empresas alojan su información no pertenecen a ellas mismas, sino al proveedor del servicio. Por lo tanto, la pérdida de control sobre los datos genera un alto grado de incertidumbre, que pone en duda la viabilidad de implementar este tipo de sistemas para aquellas organizaciones que se preocupan por la seguridad. Algunos de los aspectos que debemos tener en cuenta cuando utilizamos este tipo de servicios son:

Utilizar encriptación de discos

Si la información almacenada en los discos rígidos no se encuentra encriptada, cualquier persona con acceso a ellos –sobre todo, en el caso de los discos virtuales– podría llegar a realizar fácilmente una copia de todos los datos que contienen. Al utilizar encriptación, hacemos que solamente el sistema operativo con las herramientas y claves adecuadas pueda leer la información, con lo cual reducimos el riesgo de una fuga de datos.



Figura 15. La plataforma **EC2**, de **Amazon**, fue una de las primeras ofertas de servicios del tipo cloud computing. Cuenta con una gran cantidad de características y una probada estabilidad (<http://aws.amazon.com/ec2>).

Asegurarnos de tener copias de respaldo de los datos

Debemos corroborar que existan copias de seguridad de nuestros datos, y que estas funcionen correctamente. Ya sea que las hagamos nosotros, o el mismo proveedor del servicio, es necesario verificar que las copias existen y pueden ser recuperadas sin problemas. Son muchos los casos en los que un malentendido llevó a pensar que el proveedor realizaba copias de seguridad, cuando en realidad no era así, y esto produjo pérdidas de datos críticos para las organizaciones.

Contratar solo a proveedores de confianza

Si vamos a utilizar este tipo de servicios para procesar información crítica, debemos contratar únicamente a proveedores de confianza, y prestar mucha atención a los acuerdos de nivel de servicio y a las políticas de seguridad y privacidad que ellos utilizan, para conocer si nuestros datos estarán verdaderamente protegidos.

La privacidad de los datos

En caso de que nos encontremos analizando si contratar o no servicios de computación en la nube, debemos considerar el tipo de datos que vamos a alojar y qué nivel de responsabilidad tenemos sobre ellos. Por ejemplo, si contratamos un software que nos permite alojar toda la información de nuestros clientes, para realizar campañas de marketing, seguimiento de ventas y otras tareas, debemos tener en cuenta qué clase de datos estaremos guardando en esta plataforma, y si las políticas de seguridad y privacidad del proveedor se adecuan a nuestras necesidades. Además, dependiendo del tipo de datos con los que trabajemos, podría llegar a ser ilegal guardarlos en los equipos de otra empresa sin notificárselo a nuestro cliente.

En los casos de datos personales, como creencias religiosas e historias médicas, que están protegidos fuertemente por la ley, debemos analizar cuidadosamente la viabilidad legal de este tipo de servicios. Por lo

tanto, ante estas situaciones, será recomendable contratar a un abogado especializado en estas cuestiones para que pueda brindarnos asistencia.

Diferencias con otros servicios

Cabe destacar que, si bien los servicios de cloud computing pueden parecer inseguros o inapropiados para cierto tipo de tareas (y no es que no lo sean), hace años que contamos con la posibilidad de contratar otros servicios de similares características, que también podrían poner en riesgo la privacidad de nuestros datos. El ejemplo más claro y evidente son los servicios de alojamiento o hosting, en los cuales una empresa guarda sus datos en los servidores del proveedor, sin tener prácticamente ningún control de lo que se hace con ellos. El peligro que puede observarse en estos casos es que el alojamiento de datos suele ser compartido con varios clientes. Si bien ellos no deberían poder acceder a la información de otro, una mala configuración de seguridad podría permitir el robo o la pérdida de datos.



Figura 16. Las grandes empresas del mercado, como **IBM**, cada vez ofrecen más servicios relacionados con la computación en la nube (www.ibm.com/cloud-computing).

Aunque los servicios de alojamiento suelen utilizarse para almacenar información pública, como los sitios web, también suelen usarse para guardar todos los correos electrónicos de una organización, por lo que se estaría dando acceso a todos los mensajes al proveedor del servicio. Debemos tener en cuenta este tipo de factores no solo para la computación en la nube, sino también para cualquier servicio que requiera alojar información en equipos ajenos a nuestra organización.

Por otra parte, servicios como el **housing** nos permiten llevar equipos de nuestra propiedad y conectarlos a la infraestructura de red de un proveedor, a fin de utilizar los recursos eléctricos, de espacio y de telecomunicaciones que este ofrece, pero sin que el proveedor tenga acceso directo a ellos. En estos casos, también es ampliamente recomendable utilizar encriptación de discos y contratar solo a proveedores de confianza.

Tecnología móvil

Las tecnologías móviles permiten aumentar enormemente la productividad de los empleados de una organización, al darles la posibilidad de trabajar desde cualquier lugar físico, conectándose a través de distintas redes de datos. Obviamente, esto trae aparejadas varias consideraciones de seguridad que debemos tener en mente si necesitamos ofrecer este tipo de conexiones. En los siguientes apartados analizaremos diversos factores para tener en cuenta.

Dispositivos portátiles

Los dispositivos portátiles, como smartphones, notebooks, tablets y otros, permiten a los usuarios transportar sus equipos de trabajo de manera sencilla, lo que les da la posibilidad de llevar sus herramientas laborales a cualquier sitio.

Cada uno de estos dispositivos suele contar con varias opciones de conectividad (como 3G, Bluetooth, y otras), que permiten a los usuarios

conectarse a distintas redes y navegar por internet. Esto genera la posibilidad de que un dispositivo conectado a nuestra red se haya conectado previamente a otras redes, que podrían no ser seguras, y que podrían haberlo infectado con algún tipo de malware.



Figura 17. Los productos de la empresa **Blackberry** se cuentan entre los dispositivos móviles más utilizados en las empresas.

En este aspecto, es de suma importancia cuidar la configuración de estos dispositivos, para evitar que los usuarios modifiquen ciertos parámetros que podrían poner en riesgo el sistema, evitar que puedan eliminar o deshabilitar los programas antimalware, etcétera.

Para estos casos se vuelven muy útiles las tecnologías como NAC (analizada en el **Capítulo 5**), que nos permiten realizar comprobaciones de los dispositivos antes de permitirles interactuar con los demás componentes de una red de datos.

A continuación, podemos ver una lista de consejos básicos para asegurar este tipo de dispositivos:

- Proteger el acceso al dispositivo mediante contraseña o huella digital.

- Utilizar solamente aplicaciones certificadas por el fabricante.
- Emplear algún software antimalware.
- No guardar datos confidenciales en estos dispositivos.

Teletrabajo

El trabajo remoto, o teletrabajo, forma parte de la política de muchas organizaciones. Se trata, básicamente, de permitir a los empleados el acceso a los recursos internos de la organización desde internet, a fin de llevar a cabo sus tareas a distancia. Esta es una opción que debemos planificar con mucho cuidado, para evitar cualquier posible brecha de seguridad. Algunas de las recomendaciones más habituales en estos casos son las siguientes:

Utilizar tecnologías de acceso VPN: esto permite que la información intercambiada entre el dispositivo remoto y los equipos que están dentro de la organización sea transportada de manera encriptada. Así, nos aseguraremos de que permitimos solo conexiones autorizadas, ya sea a través de usuario y contraseña, certificados digitales o autenticación multifactor.

Limitar los recursos accesibles desde internet: debido a que no es necesario que los empleados accedan a todos nuestros recursos a través de internet, debemos asegurarnos de permitir el acceso solo a aquellos que sean estrictamente necesarios para realizar tareas laborales puntuales.



PÉRDIDA O ROBO



Uno de los problemas más recurrentes en el uso de dispositivos portátiles es su pérdida o robo. Para protegernos contra estos peligros, debemos asegurarnos de realizar copias de seguridad de los datos que contienen, y encriptar la información que almacenan a fin de dificultar su lectura por parte de terceros.

Podemos hacer esto separando una red dedicada a estos servicios (similar a lo que ocurre en una DMZ).

Mantener las conexiones en el mínimo posible: debemos mantener la cantidad de equipos y usuarios que pueden realizar conexiones a nuestra red desde internet en el número más bajo posible.



Figura 18. La gran oferta de computadoras portátiles y la velocidad de los enlaces a internet han fomentado la implementación del **teletrabajo** como práctica común en muchas empresas.



Ataques dirigidos

En la mayoría de los casos, los **ataques** a las organizaciones suelen estar hechos por personas que buscan servicios públicos mal configurados o que están probando alguna nueva herramienta de seguridad. Ya sea que se trate de profesionales con amplios conocimientos o de personas que solo

están motivadas por un momento de curiosidad, los ataques suelen hacerse a cualquier sistema que cuente con alguna vulnerabilidad conocida. Esto hace necesario efectuar varias pruebas sobre un sistema (generalmente, con herramientas automatizadas), de modo que si este no presenta fallencias, se proceda a buscar otro distinto para atacar.

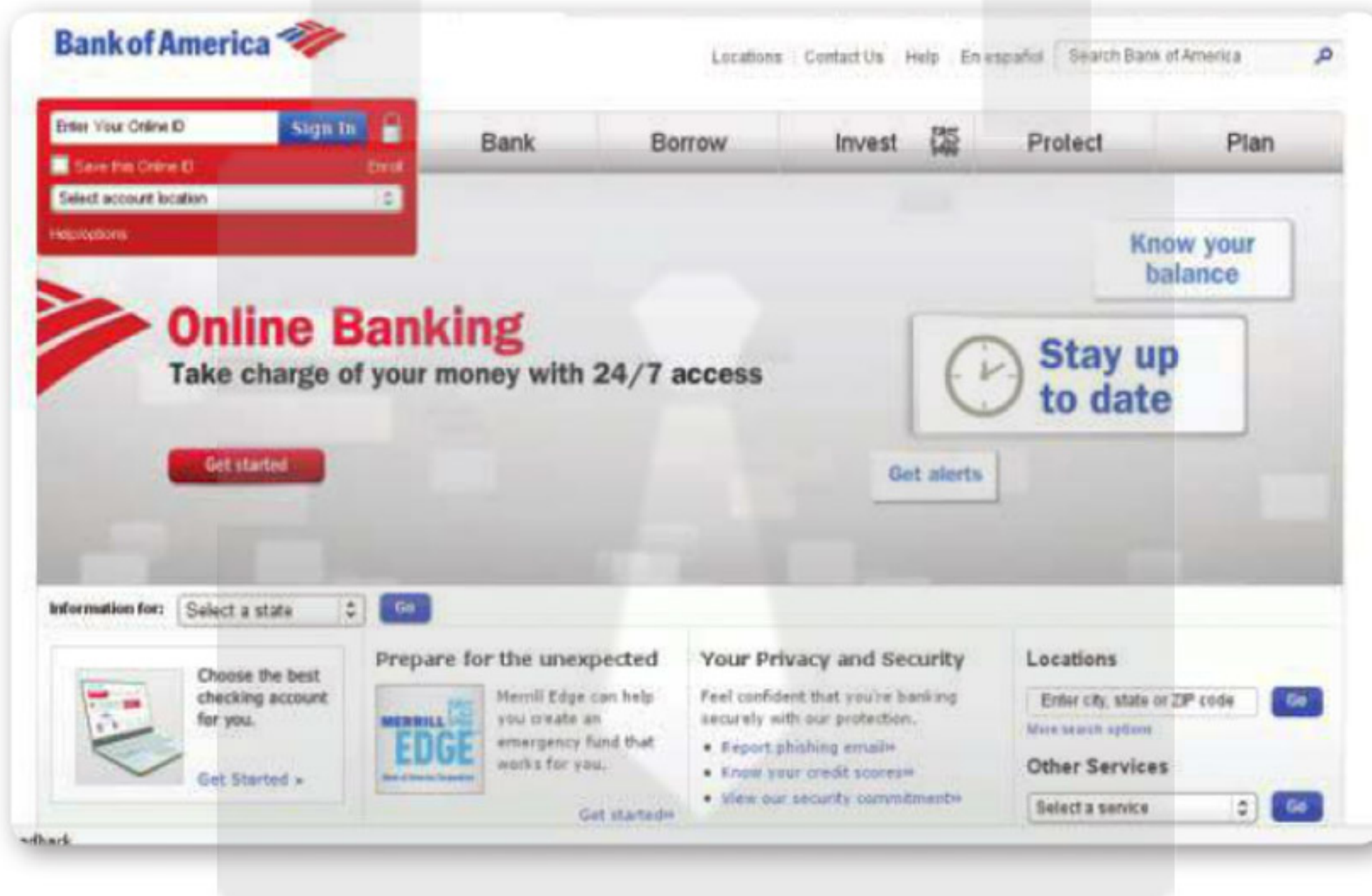


Figura 19. Las **instituciones financieras** de todo el mundo suelen ser el objetivo de ataques, por representar una potencial ganancia de dinero si se consigue vulnerar su plataforma de **banca en línea**.

Pero existe otro tipo de ataques, en los que se define un objetivo único y se lo intenta atacar constantemente, de una manera u otra, mediante distintas técnicas y herramientas. Estos ataques en general están dirigidos a entidades financieras o a organizaciones reconocidas, con el objetivo de crear pánico o como un modo de protesta.

La gran diferencia que presentan los ataques dirigidos es que, como profesionales de la seguridad, debemos enfrentarnos con la perseverancia de los atacantes y, a veces, con una gran cantidad de ellos, lo que hace que la acción resulte mucho más peligrosa y dañina.

Denegación de servicio (DoS)

En general, los ataques del tipo **protesta** tienen que ver más con generar una **denegación de servicio** (DoS, *Denial of Service*), que con robar o destruir información. Esto suele ser así porque generar un DoS suele ser relativamente sencillo si se cuenta con una cantidad suficiente de atacantes. La idea detrás de este método es agotar todos los recursos del sistema, para que este quede imposibilitado de responder a las peticiones de clientes legítimos.

Si somos los encargados de asegurar una infraestructura de servicios que podría ser víctima de esta clase de peligro, deberemos tomar los recaudos necesarios e implementar los filtros correspondientes para evitar que nuestros servicios dejen de responder.

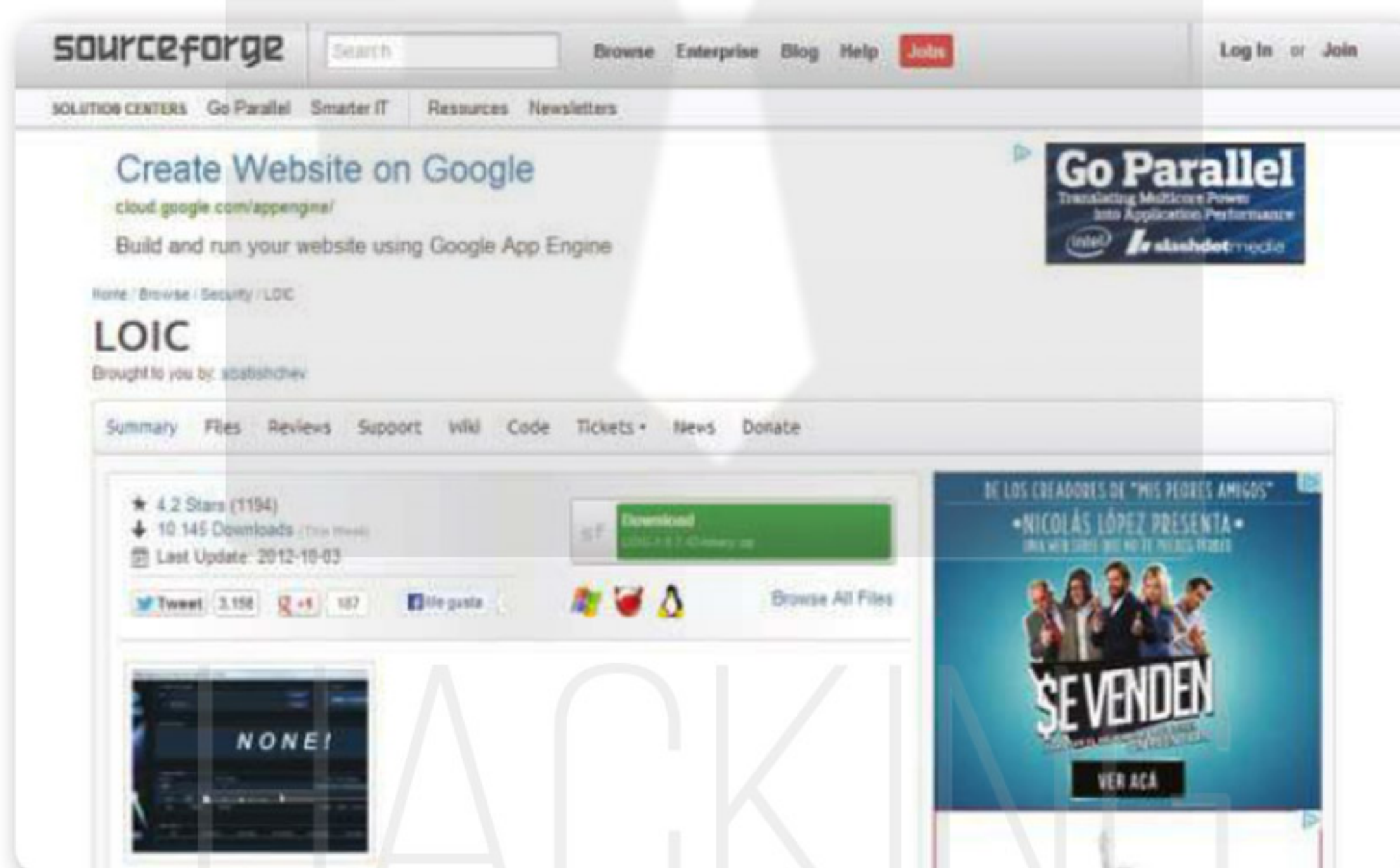


Figura 20. La herramienta **LOIC (Low Orbit Ion Cannon)** fue desarrollada, originalmente, para realizar pruebas de stress sobre servidores, pero muchos atacantes la han usado para efectuar denegaciones de servicio (<http://sourceforge.net/projects/loic>).

En el caso de los ataques DoS o los ataques distribuidos de DoS (DDoS), la forma más eficiente de protegernos es restringir la cantidad de conexio-

nes que un mismo cliente puede realizar hacia nuestro servidor, bloqueando cualquier conexión que exceda esos límites. Esto puede llevarse a cabo fácilmente si contamos con un firewall, ya sea un dispositivo especializado o alguna de las soluciones de código abierto basadas en sistemas UNIX.

Con los tres comandos que figuran a continuación, podemos utilizar el filtrado **IPTables** de los sistemas **Linux** para proteger las conexiones realizadas al puerto TCP/80 de nuestro equipo. Esto permitirá solo seis conexiones por minuto, lo cual restringe, principalmente, los ataques de tipo DoS. Por supuesto, habrá que ajustar estos valores de acuerdo con nuestros requerimientos.

```
iptables -A INPUT -p TCP -m state --state NEW --dport 80 -m recent --set
iptables -A INPUT -p TCP -m state --state NEW --dport 80 -m recent --update
--seconds 60 --hitcount 7 -j DROP
iptables -A INPUT -p TCP -m state --state NEW --dport 80 -j ACCEPT
```

Debido a que los ataques del tipo DoS son muy fáciles de realizar, debemos estar preparados para responder en forma adecuada.

El peligro de la perseverancia

Cuando estamos administrando los sistemas de una entidad que puede ser de gran interés para los atacantes –generalmente, por cuestiones económicas, políticas o militares–, debemos tener en cuenta que no solo nos enfrentamos con ataques superficiales, sino que también podríamos ser el objetivo de varias semanas o meses de intentos de intrusión. Esto nos obliga a estar preparados de manera adicional, y a implementar varias tecnologías para la detección temprana de los ataques, que nos permitan bloquearlos antes de que causen cualquier tipo de daños a nuestra infraestructura.

Para estos casos, los sistemas de detección de intrusos serán un aliado fundamental en nuestra lucha contra los atacantes, porque nos permiten reaccionar de forma proactiva.



Expectativas para el futuro

La seguridad informática, como profesión y como mercado, avanza constantemente. Es cada vez más evidente la importancia de la información en los negocios actuales, y eso lleva a las organizaciones a implementar medidas de seguridad como parte de sus procesos de negocio. De la misma forma, la aparición de nuevas tecnologías impulsa la evolución de las técnicas de seguridad, que necesitan contrarrestar la gran cantidad de malware y herramientas de ataque que se generan día a día.

Todas las tecnologías mencionadas en este capítulo están relacionadas entre sí, de una u otra forma. Las comunicaciones se unifican en las redes IP, para transmitir voz, video y datos a través del mismo medio. Esto permite abaratar costos y crear nuevas funcionalidades, que se apoyan en la movilidad de los dispositivos portátiles y el constante crecimiento en las velocidades de transferencia.

La Web se acerca cada vez más al usuario, y lo tiene como protagonista principal: ahora deja de ser un simple lector, y pasa a ser un ente de interacción, con las redes sociales y los servicios de mensajería instantánea, que buscan mantener a las personas constantemente en contacto unas con otras. Sumado a que actualmente existen muchas estafas electrónicas dirigidas a los usuarios, esto hace que cada día cada individuo deba ser más responsable para no resultar víctima de ataques y robos de información, así como también para no convertirse en el puente que facilite el acceso a datos confidenciales de una entidad.

Debido a la gran demanda de tráfico y a la enorme cantidad de usuarios de internet, muchos servicios migran a una arquitectura de cloud computing, y son numerosas las empresas que cuentan con sus propias nubes, formadas por servidores distribuidos a través del planeta. Esta tendencia



de llevar nuestra información a servidores de otras empresas hace que debamos tomar recaudos particulares en cuanto a qué información subimos a la nube y cuánto confiamos en las compañías que se ocupan de brindarnos estos servicios.

Desde el punto de vista económico, las empresas no pueden darse el lujo de invertir en todos los aspectos relacionados con la seguridad, porque el presupuesto para la adquisición de software, hardware y servicios es muy limitado y debe administrarse estratégicamente. Es por eso que, como profesionales, debemos estar a la altura de las circunstancias y tener la capacidad de recomendar en qué se debe invertir para proteger adecuadamente los activos de una organización.

También debemos buscar la capacitación constante, para mantenernos vigentes en nuestra profesión.

Un experto en seguridad informática deja de ser un simple empleado, y pasa a ser una persona que tiene un valor muy alto en el mercado. Debemos aprovechar esta situación y hacer nuestro mejor esfuerzo por mantenernos en la elite de los profesionales, característica que es muy bien recompensada en la actualidad.



RESUMEN



Gracias a los conceptos que profundizamos en este capítulo pudimos conocer las tendencias tecnológicas actuales, para, de esta forma, estar preparados ante los riesgos en la seguridad que se nos presentan. Vimos las características de la Web 2.0 y mencionamos los servicios más utilizados por los usuarios, así como también los peligros de seguridad que es necesario considerar. Analizamos los servicios de mensajería y conocimos las características de la comunicación VoIP. Examinamos los aportes y riesgos de la virtualización y de los servicios de cloud computing. Finalmente, nos detuvimos en las tecnologías móviles y conocimos el peligro de los ataques dirigidos.

Actividades

TEST DE AUTOEVALUACIÓN

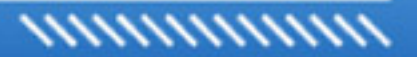
- 1 ¿Qué es un ataque de phishing y cómo puede prevenirse?
- 2 ¿Cómo podemos protegernos del Google hacking?
- 3 ¿Cómo podemos evitar el espionaje de comunicaciones VoIP?
- 4 ¿Qué debemos considerar al adquirir un servicio de cloud computing?
- 5 ¿Cómo podemos defendernos de los ataques del tipo DoS?



PROFESOR EN LÍNEA



Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: **profesor@redusers.com**



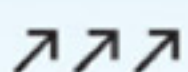
Servicios al lector

En esta sección incluimos un completo índice temático para encontrar, de manera sencilla, los conceptos fundamentales que se encuentran presentes en el libro.



HACKING
LATAM

• Índice temático184



Índice temático

A

Aceptar	50
Alineamiento a futuro	151
Ambientes de prueba.....	77
Amenazas	43
Análisis cualitativo.....	41
Análisis cuantitativo.....	41
Análisis de logs	167
Análisis de seguridad.....	36
Archivos críticos.....	74
ARP	93
Arpalert.....	93
Arpwatch.....	38
Ataques de malware	74
Auscert.....	145
Autenticación centralizada	148
Autenticación fuerte.....	108
Autenticación multifactor	160
Autoconocimiento	37

B

Backups	157
Bácula	67
BCP.....	81
BIA	81
Biometría	164

C

Caídas de servicio	151
Cambios necesarios.....	151
Capacitación al personal	60
CEH	18
Certificaciones.....	17

C

CISA	18
Cisco Systems	96
CISM.....	18
CISSP	18
Clasificar activos	40
CLI.....	117
COCI.....	100
Cold site	87
Confidencialidad.....	43
Configuración de dispositivos	97
Configuración remota.....	99
Contingencia	87
Continuidad del negocio	66
Contramida	45
Control de cambios.....	74
Copias de respaldo	67
Cuentas centralizadas	100
Cuota de mercado	142

D

Defensa en profundidad.....	20
Desarrollo de un BCP.....	86
DeviceExpert.....	75
DHCP Snooping	100
Diameter	102
Disponibilidad	43
DMZ.....	130
DNS	126
DRI Internacional	82
DRP	81

E

Enfoque en capas	20
Equipo de seguridad.....	58
Estado de encriptación.....	74
Estandarización	14
Ettercap	93

F

Filtrado de conexiones	147
Firewalls.....	103
FIRST	81
Fortinet	104
FTP	123

G

Gestión de incidentes	78
Gestión de parches	181
GUI	117

H

Hardening	144
Hispasec	16
Hot site.....	87
HTTP	123

I

IBM Trivoli	118
IDS.....	111
IMAP	122
Implementación de controles.....	49
Inteco	60
Integridad.....	43
Inventario de dispositivos	93
IPS.....	111
IronMountain.....	70
ISO.....	14
ISO27000	14
ISO27005	37

L

Lista de MAC	98
Logs	148

M

Malware	152
Mantis	78
Mejora continua.....	32
Metodologías de trabajo.....	19
Métricas de seguridad	30
Microsoft.....	141
Modificar claves.....	108
Modificar SSID.....	108
Monitoreo.....	71

N

NAC	150
Nagios	72
NAP	150
Navaja de Ockham	23
Nessus	48
No publicar SSID.....	108
NSA	21

O

Objetivos.....	24
OCS Inventory.....	39
OCTAVE	36
OCTAVE-S.....	36
OpenSSH	120
Operaciones	22
OSSIM	80

P

PandoraFMS	73
Particiones de disco	148
Personas.....	21
Política de contraseñas	146

E

Enfoque en capas	20
Equipo de seguridad.....	58
Estado de encriptación.....	74
Estandarización	14
Ettercap	93

F

Filtrado de conexiones	147
Firewalls.....	103
FIRST	81
Fortinet	104
FTP	123

G

Gestión de incidentes	78
Gestión de parches	181
GUI	117

H

Hardening	144
Hispasec	16
Hots ite.....	87
HTTP	123

I

IBM Trivoli	118
IDS.....	111
IMAP	122
Implementación de controles.....	49
Inteco	60
Integridad.....	43
Inventario de dispositivos	93
IPS.....	111
IronMountain.....	70
ISO.....	14
ISO27000.....	14
ISO27005.....	37

L

Lista de MAC	98
Logs	148

M

Malware	152
Mantis	78
Mejorac ontinua.....	32
Metodologías de trabajo.....	19
Métricas de seguridad	30
Microsoft.....	141
Modificar claves.....	108
Modificar SSID.....	108
Monitoreo.....	71

N

NAC	150
Nagios	72
NAP	150
Navaja de Ockham	23
Nessus	48
No publicar SSID.....	108
NSA	21

O

Objetivos.....	24
OCS Inventory.....	39
OCTAVE	36
OCTAVE-S.....	36
OpenSSH	120
Operaciones	22
OSSIM	80

P

PandoraFMS	73
Particiones de disco	148
Personas.....	21
Política de contraseñas	146

P

POP3.....	122
Port Security	93
Prelude.....	79
Prevención de intrusos	110
Principio de parsimonia.....	23
Principio KISS.....	22
Proceso de negocio	27
Protección en capas	154
Protocolos TCP/IP	119
Puertos abiertos	178
Puppet.....	76
Python.....	28

R

Radius	102
RANCID	116
Recursoshum anos.....	61
Redes de computadoras.....	92
Redes inalámbricas	106
Redes seguras	130
Registros	148
Responsabilidades	57
Riesgo	45
Routers.....	96

S

SANS	54
Scrapy	94
Scripting.....	94
Scripts.....	96
Security+	18
Separaciones de red.....	133
Servicios utilizados	145
Servidor.....	133
Servidores centralizados	168

S

Servidores syslog	102
SIEM	79
Sistema actualizado	146
Sistema de detección de intrusos	111
Sistemas operativos	140
Sistemas UNIX	143
Sistemas Windows.....	142
Sitios de contingencia	86
SMTP.....	122
SNMP	128
Solarwinds.....	173
Solución de monitoreo.....	75
SSH.....	120
Superespecialización.....	17
Switches	93,96

T

TACACS+	101
Tecnologías de storage	17
Tiger	148
TLS	121
Trap SNMP	93
TUI	117

U

UltraVNC	174
UNIX.....	141
Utilizar WPA/WPA2	110

W

Webmin	176
Wireshark.....	93
WMI.....	172
WUI	117