GUÍA RÁPIDA FRANCIS LEFEBVRE

Ciberseguridad para Despachos y Profesionales

Fecha de edición: 27 de noviembre de 2018

Es una obra realizada por iniciativa
y bajo la coordinación
de la Redacción de
Francis Lefebvre
sobre la base de un estudio técnico
cedido por

Autores:

JOSÉ MIGUEL CARDONA PASTOR
Ingeniero de Telecomunicación. Socio de Auren.
JOSEP SALVADOR CUÑAT FERRANDO
Ingeniero de Telecomunicación. Socio de Auren.

Colaboradores:

JORGE GARCÍA PERALES
Ingeniero de Telecomunicación. Socio de Auren.
DAVID IRIBAS RAZQUIN
Consultor Tecnológico. Socio de Auren.
ALEJANDRO DAPIA GÓMEZ
Ingeniero de Telecomunicación. Gerente de Auren.
ANTONIO SÁNCHEZ ARAGÓ
Ingeniero Técnico en Informática. Consultor de Auren.
JUAN TÁRREGA ALONSO
Ingeniero de Telecomunicación. Consultor de Auren.
VICENT SIGNES PEDRÓS
Ingeniero de Telecomunicación. Consultor de Auren.
JORGE SÁNCHEZ ESTEBAN
Ingeniero de Telecomunicación. Consultor de Auren.
DANIEL LÓPEZ ORTIZ
Ingeniero de Telecomunicación. Consultor de Auren.
JOSÉ MANUEL BARRIOS FERNÁNDEZ
Ingeniero en Informática. Gerente de Auren.
JUAN FRANCISCO ESCUDEROS LÓPEZ
Ingeniero de Telecomunicación. Director de Auren.
VICENTE CHIVA CARBONELL
Ingeniero en Informática. Director de Auren.
BORIS DELGADO RISS
Ingeniero en Informática. Gerente de TIC. AENOR.
CARLOS MANUEL FERNÁNDEZ SÁNCHEZ
Ingeniero en Informática. MBA. Asesor Estratégico de TI. AENOR.
ANTONIO SERRANO LAHIGUERA
Consultor. Gerente de Auren.

Lefebvre-El Derecho, S. A.
Monasterios de Suso y Yuso, 34. 28049 Madrid. Teléfono: (91) 210 80 00. Fax: (91) 210 80 01
www.efl.es
Precio: 39,52 € (IVA incluido)

ISBN: 978-84-17544-34-8
Depósito legal: M-39434-2018

Impreso en España
por Printing'94
Paseo de la Habana, 9-11. 28036 Madrid

Plan general

Abreviaturas

AAPP:	Administraciones Públicas
AARR:	Análisis de Riesgos
AEPD:	Agencia Española de Protección de Datos
ANS:	Acuerdo de Nivel de Servicio *(Service Level Agreement)*
API:	*Application Programming Interface*
APT:	Amenazas Persistentes Avanzadas *(Advanced Persistent Threat)*
art.:	artículo/s
BBDD:	Bases de Datos
BIA:	*Business Impact Analysis*
BYOD:	*Bring Your Own Device*
CA:	Autoridad de Certificación (*Certification Authority*)
ccTLD:	*country code Top-Level Domain*
CDE:	*Cardholder Data Environment*
CERT:	Equipo de Respuesta ante Emergencias Informáticas *(Computer Emergency Response Team)*
CHD:	*CardHolder Data*
CM:	*Community Manager*
CPS:	Declaración de Prácticas de Certificación (*Certification Practice Statement*)
CRL:	Lista de Certificados Revocados *(Certificate Revocation List)*
CRM:	*Customer Relationship Management*
CSIRT:	Equipos de Respuesta a Incidentes de Seguridad *(Computer Security Incident Response Team)*
CSV:	Código Seguro de Verificación
DDoS:	Ataque de Denegación de servicio distribuido *(distributed DoS)*
Dir:	Directiva
DLT:	Tecnologías de Registro Distribuidos *(Distributed Ledger Technology)*
DMZ:	Zona desmilitarizada (*DeMilitarized Zone*)
DNIe:	Documento Nacional de Identidad Electrónico
DNS:	*Domain Name Server*
DoS:	Denegación de servicio *(Denial of Service)*
DRP:	Plan de Recuperación de Desastre (*Disaster Recovery Plan*)
EDJ:	El Derecho Jurisprudencia
eIDAS:	Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (*Electronic IDentification And trust Services for electronic transactions*)
ENI:	Esquema Nacional de Interoperabilidad
ENISA:	Agencia Europea de Seguridad de las Redes y de la Información *(European Union Agency for Network and Information Security)*
ENS:	Esquema Nacional de Seguridad
ETH:	Ethereum (criptomoneda)
GSM:	*Global System for Mobile Communications*
HIDS:	*Host Intrusion Detection System*
HTML:	*HyperText Markup Language*
HTTP:	Protocolo de Transferencia de Hipertexto *(Hypertext Transfer Protocol)*
HTTPS:	*HyperText Transfer Protocol Secure*
ICANN:	Corporación para la Asignación de Nombres y Números en Internet *(Internet Corporation for Assigned Names and Numbers)*
ICO:	Oferta Inicial de (Cripto)Monedas (*Initial Coin Offering*)

IDS:	Sistemas de Detección de Intrusiones *(Intrusion Detection System)*
IMAP:	*Internet Message Access Protocol*
IP:	*Internet Protocol*
ISO:	Organización Internacional de Normalización (*International Organization for Standardization*)
ISP:	Proveedores de Servicios de Internet *(Internet Service Provider)*
ISSAF:	*Information Systems Security Assessment Framework*
L:	Ley
LAN:	*Local Area Network*
LO:	Ley Orgánica
LOPD:	Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999)
MAN:	*Metropolitan Area Network*
MDM:	*Mobile Device Management*
MIME:	*Multipurpose Internet Mail Extension*
MITM:	*Man In The Middle*
NGFW:	*Next Generation FireWall*
NIDS:	*Network IDS*
NIST:	Instituto Nacional de Estándares y Tecnología *(National Institute of Standards and Technology)*
OMPI:	Organización Mundial de la Propiedad Intelectual
OPV:	Oferta Pública de Valores
OSINT:	*Open Source Intelligence*
OSSTMM:	*Open Source Security Testing Methodology Manual*
OWASP:	*Open Web Application Security Project*
PBC:	Prevención del blanqueo de capitales *(AML-Anti-Money Laundering).*
PCI DSS:	Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago *(Payment Card Industry Data Security Standard)*
PCN:	Plan de Continuidad de Negocio
PDCA/PHVA:	Ciclo de Deming
PII:	Información Personal Identificable (*Personally Identificable Information*)
PKI:	Infraestructura de Clave Pública (*Public Key Infrastructure*)
POP:	Protocolo de Oficina Postal
PSC:	Prestador de Servicios de Certificación
PTR:	Plan de Tratamiento de Riesgos
QSCD:	*Qualified Signature Creation Device*
RA:	Autoridad de Registro (*Registration Authority*)
RD:	Real Decreto
RDL:	Real Decreto Ley
RGPD:	Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Rgto UE/2016/679)
Rgto:	Reglamento
RPA:	Automatización Robótica de Procesos (*Robotic Process Automation*)
RPO:	*Recovery Point Objective*
SaaS:	*Software as a Service*
SAD:	*Sensitive Autentication Data*
SAI:	Sistema de Alimentación Ininterrumpida *(Uninterruptible Power Supply/Source)*
SEO:	*Search Engine Optimization*
SGC:	Sistema gestión de calidad (Norma ISO 9001)
SGSI:	Sistema de gestión de seguridad de la información (Norma ISO 27001)
SGSTI:	Sistema de gestión de servicios de TI (Norma ISO 20000)
SMS:	*Short Message Service*
SMTP:	*Simple Mail Transfer Protocol*
SO:	Sistema Operativo
SOC:	Centro de Operaciones de Seguridad *(Security Operation Center)*

SSO:	*Single Sign-On*
TI:	Tecnologías de la Información
TIC:	Tecnologías de Información y Comunicación
TJUE:	Tribunal de Justicia de la Unión Europea
TLD:	Dominio de Nivel Superior *(Top Level Domain)*
TLS:	*Transport Layer Security*
TOR:	*The Onion Router*
TSA:	Autoridad de Sellado de Tiempo (*Time Stamping Authority*)
TSL:	Lista de Confianza de Prestadores Cualificados de Servicios Electrónicos de Confianza *(Trust Service List)*
UE:	Unión Europea
URL:	*Uniform Resource Locator*
UTM:	Gestión Unificada de Amenazas *(Unified Thread Management)*
VA:	Autoridad de Validación (*Validation Authority*)
VLAN:	*Virtual Local Area Network*
VPN:	Redes Privadas Virtuales *(Virtual Private Network)*
WAN	*Wide Area Network*
WiFi:	*Wireless-Fidelity*
WLAN:	*Wireless Local Area Network*
WMAN:	*Wireless Metropolitan Area Network*
www:	*World Wide Web*

Introducción

La presente obra pretende mejorar sus conocimientos sobre ordenadores, redes, aplicaciones e internet, todo ello enfocado desde el punto de vista de la seguridad de la información y de la ciberseguridad como subcomponente de esta. Para el desarrollo de este se ha tenido en cuenta que, en general, el público de esta obra será aquel vinculado a un despacho profesional con los recursos realistas de los que se pueda disponer habitualmente en ese contexto, proporcionando orientaciones y guías de alto nivel, pero sin ahondar en vericuetos técnicos para su mejor comprensión.

La **motivación** de esta obra está más que justificada dada la absoluta dependencia de los sistemas de información, y por ende de la seguridad de estos, que tienen prácticamente todas las organizaciones para su operativa, bien sean públicas o privadas, yendo desde grandes multinacionales a pymes, gobiernos e incluso para los propios usuarios individuales ya fuera de un marco empresarial. Incluso de manera más amplia, la ciberseguridad juega un papel clave para la sociedad y todos nosotros como ciudadanos, para mantener nuestro estado de bienestar y estilo de vida, y a raíz de ello se han ido desarrollando cada vez más normativas y regulaciones en este sentido a nivel internacional, dada su absoluta relevancia.

Cualquier **despacho profesional** depende de la tecnología para: prestar sus servicios, almacenar su información (propia y de sus clientes), mantener contacto con los mismos, ofrecer sus servicios a posibles nuevos clientes, tener presencia en el mercado, disponer de entornos para intercambiar información a nivel interno o externo, disponer de instrumentos de obtención de información y consulta, disponer mecanismos de comunicación con organizaciones públicas y entes reguladores y un largo etc.

En resumen, cualquier despacho profesional requiere de **tecnología y sistemas de información**, y de manera inherente a estos, por su propia idiosincrasia, requiere de la **protección** de estos, ya que cualquier sistema por definición es inseguro en un determinado momento del tiempo y ha de ser protegido. Es decir, seamos conscientes o no, la ciberseguridad es un aliado invisible pero imprescindible que se ha de aplicar a distintos niveles y sobre distintos elementos en el ecosistema de un despacho profesional, ya empleando términos bélicos, dejar un solo flanco sin cubrir supondrá con alta certeza la pérdida de la batalla, al igual que una fuga de agua en el caso de un barco, terminará suponiendo que este se llene de agua e irremisiblemente se hunda.

A lo largo de los diferentes capítulos se exponen los conceptos y fundamentos, así como **sugerencias y recomendaciones** de cómo mejorar la ciberseguridad de la información que maneja de forma diaria a través de su ordenador, teléfono móvil, tableta, red corporativa, etc. Complementariamente se exponen los posibles riesgos a los que se enfrenta si no siguen esas pautas y cómo pueden afectar estos a su negocio.

A modo ejemplo:

Conocerá de esa forma, cómo proteger los datos que envía a través de **correo electrónico**, para poder protegerse mejor frente a los intentos de fraude que utilizan técnicas de **Phising** (o suplantación de identidad) (Capítulos 4 y 7).

Tendrá criterios más sólidos y fundamentados para elegir cómo compartir información con sus colaboradores en la **nube** (repositorios y servicios de datos en internet) y que le garantice unos mejores niveles de confidencialidad y disponibilidad para su negocio, más allá del mero criterio de coste, marca o funcionalidad (Capítulo 10).

Sabrá, con más elementos de juicio, si una **página web de comercio electrónico** es o no todo lo segura que debería ser, así como la importancia de su reputación en internet (Capítulo 9).

También le indicaremos cómo plantear un **plan de continuidad de negocio** para que tenga previstas las actuaciones en caso de ocurrir un incidente, como fallo de instalaciones, personas, comunicaciones, programas o sistemas informáticos y cómo responder ante ellos (Capítulo 5).

Conocerá aquello que se debe tener en cuenta para que las **aplicaciones corporativas** mejoren en cuanto al nivel de ciberseguridad de estas (Capítulo 6).

Se expondrán prácticas recomendadas para el buen uso de los **dispositivos móviles** (Capítulo 8).

Aprenderá qué directrices debe seguir para mejorar evitar instalar ***malware*** en sus equipos y mejorar la seguridad de su red (Capítulos 2 y 3).

Le contaremos la tecnología que sustenta las **criptomonedas** como el **Bitcoin** y qué utilidad puede tener en otros ámbitos, así como nuevas tendencias en tecnología y su impacto en la ciberseguridad, y un largo etc. (Capítulos 13 y 14).

Conocerá los usos y aplicaciones de la firma electrónica y los principales estándares y normativas relacionados con la ciberseguridad (Capítulos 11 y 12).

Para ello, empezaremos primero sentando unas mínimas bases de conocimiento sobre **redes de telecomunicaciones**, programas informáticos y por supuesto sistemas de información como ordenadores personales y dispositivos móviles. De esa forma podrá comprender mejor los fundamentos de estas tecnologías y cómo pueden protegerse (Capítulo 1).

CAPÍTULO 1

Introducción al funcionamiento de internet y a la ciberseguridad

1. Estructura básica de los ordenadores y redes

Se va a indicar, de forma genérica y muy conceptual, **cómo funciona un ordenador**. La mayoría de los componentes básicos están presentes también en cualquier tipo de dispositivo electrónico que utilizamos de forma habitual. Es decir, aunque no tengan las mismas prestaciones, tamaño o aspecto físico, forman parte de nuestro teléfono inteligente o nuestra tableta de forma parecida a un ordenador, estando integrados en el mismo.

Se pueden agrupar los **componentes** de los ordenadores en dos partes:

a) La parte física o **hardware** compuesta en el caso de un ordenador portátil por su pantalla, teclado, procesador, memoria, disco duro, etc.

b) Estos componentes son los encargados de que el **software** o programas funcionen sobre nuestro equipo y se pueda de esa forma utilizar, por ejemplo: navegadores web, programas de correo, aplicaciones de gestión de expedientes, procesadores de texto, hojas de cálculo, etc.

A nuestros equipos informáticos se les puede acoplar distintos **periféricos**, como teclados expandidos, tarjetas de sonido, lectores o grabadores de discos ópticos o tarjetas de memoria, ratones, discos duros extraíbles, impresoras, etc. con la finalidad de ampliar funcionalidades y usabilidad.

Evolución histórica Al inicio de la aparición de los ordenadores, estos se encontraban en entornos aislados, es decir sin conexión con otros ordenadores, sin conexión a internet y en general sin interacción con otros dispositivos. Hoy en día esta situación no es la habitual, sino todo lo contrario y se comprenden fácilmente las ventajas (ya convertida en necesidad) de **compartir información** con otras personas, instituciones, empresas, etc.

Es por ese motivo por lo que se desarrollaron en primera instancia las **redes locales** que conseguían que los diferentes ordenadores que estaban ubicados relativamente cerca pudieran conectarse entre ellos compartiendo algún recurso, como por ejemplo un disco duro, donde almacenar información común o un servidor que ofreciera un programa común instalado en él a todos los puestos de usuario cercano para facilitar la gestión de la información, etc.

A partir de la extensión de las redes locales y la comprobación de su utilidad, se vislumbró la posibilidad de **conectar las diferentes redes locales** de las empresas o instituciones entre sí. El razonamiento fue que si era útil conectar ordenadores relativamente cercanos, también lo sería que los terminales de las diferentes oficinas que estaban separadas por kilómetros o incluso en extremos opuestos de un país se pudieran comunicar de alguna forma.

Con la idea comentada, apareció el **embrión de internet**, una red que se denominaba **ARPANET**. En el año 1971 solamente había 21 ordenadores conectados. ¿Pero cómo funcionaba esta red y qué posibilidades ofrecía?

Concepto de arquitectura cliente/servidor Para entender los conceptos anteriores y de cómo aún hoy en día funcionan muchos sistemas, se ha de revisar el concepto de arquitectura cliente/servidor.

Esta apareció como consecuencia de las primeras redes locales y la capacidad de conectar diferentes ordenadores que se encontraban relativamente cerca. Imaginemos una oficina en la que se gestiona la contabilidad de una empresa. Para poder abordar todo el conjunto de tareas, son necesarias varias personas que se encarguen de la introducción de datos. Una de las soluciones la ofrece la arquitectura cliente/servidor. En un equipo, denominado servidor, se aloja o ejecuta el programa de contabilidad central, capaz de atender todas las peticiones de los diferentes clientes conectados a él.

1. Se denomina **cliente** al programa que se ejecuta en el ordenador del usuario. Los clientes estarían funcionando en los ordenadores del personal de la oficina, teniendo este programa la capacidad para comunicarse con el programa servidor para indicar los cambios o nuevas entradas de contabilidad, pero no de almacenar los datos.
2. La función del almacenamiento de datos, puesto que debe estar actualizado y no depender de un único usuario, está delegada en el **servidor**. De esa forma, la información se centraliza por un único equipo, que está dedicado a la función de controlar el funcionamiento de la contabilidad, siguiendo con el ejemplo anterior, y, en caso de conflicto de datos, podría gestionar la recuperación puesto que dispone de las últimas modificaciones introducidas por los usuarios a través de los programas clientes.

Esta es la filosofía de la arquitectura cliente/servidor, donde la **información** se maneja de forma **centralizada** y los cambios o consultas pueden realizarse desde muchos ordenadores de manera simultánea.

Otra ventaja de la arquitectura cliente/servidor se puede comprender, si, por ejemplo, en algún momento el ordenador del usuario deja de funcionar, la información introducida a través del programa cliente de contabilidad quedaría almacenada en el servidor. Esta ventaja por supuesto puede convertirse en una debilidad puesto que, si se perdiera la información del servidor, se perdería toda la información; pero por contra, facilita el hacer **copias de seguridad** (lo que mitigaría este riesgo, tal y como se explica en el capítulo 5).

Siguiendo con la evolución de internet, para poder interconectar más de dos dispositivos de forma simultánea se tuvo que diseñar, probar e implementar unos protocolos de comunicaciones. Estos, en esencia, son normas o reglas para las **conversaciones digitales**, es decir, conversaciones entre equipos digitales compuestas por mensajes.

Los mensajes los lanzan los ordenadores individuales y pueden estar dirigidos para que los interprete directamente un servidor o para que lleguen a otro ordenador de usuario.

Normalmente, aunque los mensajes estén pensados para transmitirse entre ordenadores de usuarios, se estaría hablando, por ejemplo, del **envío de ficheros a través de FTP**. Incluso en estas situaciones hace falta un servidor y usar la arquitectura cliente/servidor.

2. Elementos y protocolos de internet

Se describen a continuación los elementos que componen una red en general e internet, de forma simplificada.

Elementos Se tienen, en primera instancia, todos los usuarios con sus diferentes dispositivos, ya sean ordenadores, teléfonos inteligentes, tabletas, etc. Estos equipos se suelen denominar **clientes**.

De manera muy sintetizada, en cualquier red o internet se encuentran:

a) **Servidores**: son los ordenadores que van a prestar servicios a los usuarios a través de los protocolos o lenguajes de comunicación que existen entre ordenadores. Sería el caso del servidor:

– presente en nuestro despacho que permite el almacenar archivos ofimáticos en carpetas; o también

– del proveedor que proporciona la aplicación de gestión de expedientes, de forma que cada empleado pueda trabajar en su ordenador conectado a esa aplicación, pero estando toda la información almacenada en ese servidor de forma centralizada.
b) ***Routers* o Enrutadores**: son los elementos encargados de conectar varias líneas de comunicaciones entre sí (y así conectar a las redes que hay tras cada línea de comunicación) con la capacidad de redirigir el tráfico de mensajes de forma adecuada, para que el mensaje llegue a su destino.
c) ***Firewalls* o Cortafuegos**: son elementos encargados de proteger el acceso entre redes (por ejemplo, entre nuestra red doméstica en nuestra oficina e internet). Usualmente en la actualidad se integran muchas veces con los routers. La mayoría de usuarios dispone en cada casa de un router-firewall para su conexión a internet.
d) ***Switches* o conmutadores**: son los elementos donde se conectan los ordenadores para compartir un cable de comunicaciones.
e) **Líneas de comunicaciones**: líneas existentes de comunicaciones que interconectan ordenadores o redes de ordenadores con otras redes.
f) **Redes de ordenadores**: conjunto de ordenadores interconectados entre sí mediante líneas de comunicaciones que terminan en enrutadores o conmutadores, con distintas topologías.
Haciendo un símil, la información o los mensajes sería como el agua de riego, que circula a través de las líneas de comunicaciones de complejas ramificaciones (tuberías o canalizaciones) siendo distribuida por puertas y compuertas (*routers* y *firewalls*) hasta llegar a distintos campos (redes) donde finalmente están los cultivos que absorberán esa agua (servidores). Obviamente este ejemplo no contempla la **bidireccionalidad de ese flujo** que sí aplica lógicamente a las redes de telecomunicaciones, pero confiamos que salvando el poco rigor científico ayude al lector a la comprensión en términos más sencillos del funcionamiento de las redes de comunicaciones e internet.

Protocolos Abundando en un aspecto de gran relevancia en este ecosistema, que es el cómo controlar el complejo tráfico y encaminamiento por internet, existen una gran cantidad de protocolos (especie de reglas o lenguajes para comunicar sistemas de información). Aquí se ve una versión muy sintetizada de los principales:
1. **Modelo de capas (TCP/IP)**: para resolver el problema de las comunicaciones a larga distancia y el problema de tener que soportar la posibilidad de que más de dos dispositivos pudiesen comunicarse entre sí de forma simultánea, se optó por solucionar las dificultades por capas. Esto originó el desarrollo del protocolo TCP/IP en el que se asigna una dirección (la famosa dirección IP compuesta por 4 bloques de hasta 3 dígitos cada uno separados por puntos, como 127.0.0.1) a cada ordenador para poder ordenar todas las comunicaciones.
2. **FTP**: utilizado para la transferencia de archivos, actualmente en desuso por la falta de seguridad en las comunicaciones.
3. **IMAP**: utilizado para acceder a los servidores de correo, desde los clientes de correo de los usuarios, con la finalidad de descargar o acceder a los mensajes.

Precisiones Existe otro protocolo, pero actualmente no se utiliza tanto: se trata del **POP**.

4. **SMTP**: el *Simple Mail Transfer Protocol*, se encarga de forma habitual de enviar los correos electrónicos de los programas de usuario.
5. **HTTP**: *Hypertext Transfer Protocol* o Protocolo de transferencia de hipertexto, es el encargado de proporcionar la conexión entre los servidores de la **www** (*World Wide Web*) o páginas de internet como comúnmente se denominan y los programas clientes tales como los navegadores web.
El protocolo sigue el esquema cliente/servidor, donde el usuario a través de su navegador solicita transacciones de información al servidor. Por ejemplo, al pinchar un enlace de la página web visitada o al abrir una nueva pestaña de navegación sobre una imagen, se está solicitando información al servidor, que una vez recibida la petición, procede a enviarla al solicitante desde el servidor y la muestra en la pantalla del usuario (cliente).

6. **HTTPS**: cómo puede deducirse, el *HyperText Transport Protocol Secure*, es la versión segura del HTTP. Se utiliza para comunicaciones seguras a través de la www. Para poder establecer los canales, se usa un **cifrado** basado en SSL/TLS. El nivel de seguridad del cifrado depende del algoritmo matemático utilizado para el cifrado y la seguridad del protocolo a la hora de establecer la comunicación. Actualmente posibilita la conexión segura, por ejemplo, a plataformas bancarias o de comercio electrónico a través de los navegadores más extendidos.

Precisiones Para estas conexiones seguras se usan certificados digitales (se explicarán en el capítulo 12).

7. **DNS**: de forma habitual, no suele escribirse directamente la dirección IP de un servidor para abrir una página WEB, utilizamos el nombre del Dominio o sitio Web, por ejemplo: www.portalweb.es.
La conversión entre el texto introducido y la dirección IP la realiza el **DNS** (*Domain Name Server*). Este protocolo realiza una asignación, a partir del nombre de dominio, entre el dominio y una dirección IP.
Los DNS se basan en una base de datos distribuida (repartida entre varios servidores) para poder localizar la correspondencia entre las direcciones IP y los nombres de dominio. De forma similar se realiza para la correspondencia entre el dominio de los correos electrónicos y la dirección IP numérica.
8. **DHCP**: es el mecanismo o protocolo que asigna las direcciones de los ordenadores en nuestro despacho. Los ordenadores usan el protocolo TCP/IP para comunicarse y se les puede asignar una dirección fija, pero se debe entonces ejercer un control para que dos ordenadores no repitan dirección, ya que entonces habría dificultades en las comunicaciones.
La otra opción es delegar en el protocolo DHCP la tarea de **asignar una dirección IP** diferente a cada ordenador, cada vez que se conecta a la red del despacho. Como, por ejemplo, cuando llegamos de una visita y enchufamos el ordenador portátil a la red o lo conectamos a la red wifi de la oficina.

Consecuencias La evolución de internet ha propiciado la aparición de múltiples servicios como las aplicaciones colaborativas, intranets, servicios en la nube, etc.
Estos nuevos usos de las tecnologías han propiciado que la ciberseguridad se deba extender y centrar en **proteger estas nuevas aplicaciones**.

Precisiones A continuación se describen los conceptos básicos de la ciberseguridad.

3. Introducción a la ciberseguridad

De modo simplificado se podría decir que la ciberseguridad, tal como su nombre indica, es un componente de la **seguridad de la información** aplicada a los ordenadores, teléfonos móviles inteligentes o smartphones, internet y todos los servicios asociados como páginas web, email, aplicaciones en la nube, etc.
Normalmente la ciberseguridad debe cubrir los siguientes **pilares básicos o dimensiones**: la integridad, la confidencialidad y la disponibilidad.

Integridad De forma similar a cuando se trabaja con documentos en papel, interesa que la información que manejamos en nuestros ordenadores se mantenga íntegra con el paso del tiempo. Esto significa que no debe alterarse ni modificarse si no se desea hacerlo y que sea completa y correcta.
Aplicar el principio de integridad a los documentos en papel significaría, por ejemplo, que una vez almacenados en los archivadores se pudiese confiar en que la próxima vez que se acceda a ellos para ser leídos, van a estar tal como fueron depositados.
Para cumplir el principio de integridad, deberían **mantenerse todas las partes del documento**, conservándose todas las páginas y, además, todas ellas deberían permanecer sin ningún cambio. No se admitiría que una página estuviera rota o se hubiese borrado o alterado un párrafo.

De forma similar, cuando se trabaja con ordenadores, se manejan informes, fotos, correos electrónicos, etc., interesa mantener la integridad de esa información. Si para cada ocasión que se guardase una **versión de un documento**, el proceso de guardar provocara la eliminación de partes de este, o que algún apartado se modificara, no podría confiarse en los equipos informáticos.
Mediante la aplicación de ciertas **medidas y controles** en el ámbito de la ciberseguridad se puede asegurar la integridad de la información para que, mediante el uso de los mecanismos previstos a tal efecto no se vea afectada esta dimensión en los datos que sean de nuestro interés.

Confidencialidad Se trata de otra dimensión a proteger. Se ha mencionado que interesa que la información mantenga su integridad. Pero si solamente garantizamos su integridad y nos olvidamos de los accesos no autorizados, no está completamente protegida.
Puede perfectamente almacenarse una **información en formato digital**, protegerla de su modificación y alteración, pero si no se la protege de lecturas no permitidas, se estará comprometiendo la confidencialidad de su contenido.
Volviendo al ejemplo del archivador de documentos en papel, si se desea que solamente un grupo de personas puedan acceder a los expedientes del archivador, se habrán tomado medidas como instalar una cerradura para evitar su apertura.
Si se desean aplicar medidas de confidencialidad en el transporte de los documentos, se habrá seleccionado quién transporta el documento, es posible que se haya transportado en un contenedor cerrado e incluso que solamente disponga de llave o el código de apertura la persona que envía y la que recibe.
Pues de forma similar en la ciberseguridad se pueden aplicar medidas para que la información y los documentos solamente sean **accesibles por quien deba tener acceso**. De esa forma:
– se puede mantener la confidencialidad y evitarse, por ejemplo, que los **correos electrónicos** sean leídos por terceros o para que las transacciones bancarias queden correctamente protegidas;
– se puede mejorar la confidencialidad del servicio en la **nube de gestión de expediente**, si es el caso; y
– mejorar por ejemplo la confidencialidad de los **suscriptores** a nuestro **boletín de noticias**, etc.
La confidencialidad está muy ligada a la privacidad, que se centra en la protección de un subtipo de información compuesta de todos aquellos datos vinculados a las personas físicas.

Disponibilidad Tan importante es mantener la información completa, sin modificaciones, o mantenerla a buen recaudo de accesos inadecuados o no autorizados como tenerla disponible, justo en el momento que se necesite y durante todo **el tiempo que se requiera** según su naturaleza.
Los equipos informáticos o digitales (y por extensión la información que almacenan, procesan o transmiten) deben estar disponibles cuando sean necesarios. Si se ha protegido nuestra información de forma excelente, y la misma no se puede alterar, y no puede ser accedida por terceros no autorizados, pero no está disponible, no se tiene esta dimensión satisfactoriamente cubierta, con todas las implicaciones que ello pueda suponer para nuestro despacho.
Imagínese la necesidad, antes de una hora, de enviar un documento a través de una plataforma electrónica para presentar la oferta del despacho a un concurso público. En este supuesto caso se ha perdido el documento, pero se recuerda que había una copia de seguridad en el servidor del despacho. Las circunstancias han permitido, por no tener las medidas de seguridad adecuadas, que una descarga eléctrica causada por una tormenta de la noche anterior dañara el servidor, no permitiendo su funcionamiento. Se ha avisado al proveedor para que acuda a la pronta reparación del servidor, pero las circunstancias no le permiten llegar a tiempo. Si no existe un **medio alternativo** que proporcione la información antes de la hora, se ha perdido el documento y no pueden restablecerse los datos del servidor a tiempo para extraer la

información necesaria, entonces se plantea un problema de disponibilidad que puede afectar en el no poder optar a un contrato, siguiendo el caso del ejemplo.

Dimensiones adicionales Se pueden considerar dos dimensiones adicionales:
1. El «**no repudio»** es la cualidad por la cual se garantiza que un documento, mensaje o más exactamente un conjunto de datos tienen un autor asignado y que se puede confiar con muy alta certeza de esta relación autor-datos.
También se puede denominar esta dimensión como «**irrenunciabilidad**». Por ejemplo, si un usuario genera un documento y lo firma digitalmente, queda ligado al mismo como su autor, y (como se verá en el capítulo 12 de Firma digital) se entiende sin género de dudas que el usuario es el autor del documento, aunque el mismo usuario lo negara posteriormente.
2. La **trazabilidad**, es la dimensión que permite conocer el **histórico de acciones** que se han procesado sobre un conjunto de datos.
Por ejemplo, imaginemos una aplicación de un hospital que cada vez que se lee, modifica o elimina una historia clínica, registra qué usuario ha desencadenado la acción, a qué hora e incluso añade datos adicionales como la parte que se insertó, o qué parte del expediente se ha consultado en concreto. Este sería un sistema con un alto grado de trazabilidad.

CAPÍTULO 2

Seguridad en redes (seguridad perimetral)

1. Cuestiones destacadas

- ✓ Hoy en día es muy importante controlar la seguridad de las redes para evitar, por ejemplo, el acceso no autorizado al servidor del despacho, bien desde el exterior o bien desde el interior de nuestra red corporativa. Si una visita, un invitado, que no deseemos que tenga acceso a cierta información confidencial, pudiera tener acceso a leer los **ficheros de nuestro servidor**, simplemente conectándose a la red por cable o por conexión wifi (conexión inalámbrica), se tendrá un problema grave de seguridad perimetral.
- ✓ Se desarrollan los conceptos relacionados con la protección de nuestra **red de comunicaciones** dentro del despacho.
- ✓ Se revisan las medidas de seguridad que se deben tener en cuenta para la conexión a internet tanto de los ordenadores de usuario como de servidores. Podría darse el caso que nuestro despacho tuviera el servidor de la página web de la empresa o el servidor de ficheros instalado en la propia empresa que permite el acceso a ciertos datos desde el exterior mediante conexiones remotas.
- ✓ Si se dispone de **acceso a internet compartido**, por parte de los ordenadores de los trabajadores y los servidores que dan servicio al exterior (página web, intranet, servidor de ficheros, etc.), se deben tener en cuenta algunas **medidas específicas**.
- ✓ Estos detalles, junto a una ampliación de la información relativa a como **se gestionan las redes de comunicaciones de ordenadores** o los métodos para realizar **pruebas de seguridad de red** o (*Pentest*/Test de intrusión), etc., se desarrollan en este capítulo.

2. Introducción

En el **inicio de la informática** los primeros sistemas ocupaban un volumen considerable y por tanto se alojaban en salas dedicadas específicamente a ellos. La entrada y salida a dicha sala se controlaba con métodos de seguridad física tradicional (vigilantes, cerraduras, etc.). En esa época los sistemas no estaban conectados entre ellos, sino que se usaban aisladamente de forma local.

Con la **evolución tecnológica**, el alcance de dichos sistemas aumentó, incorporando nuevos equipos en el resto de las instalaciones, de modo que, si bien los equipos de procesado de información seguían alojados en una sala de procesado o cómputo dedicada exprofeso a tal fin, a su vez se incorporaban **equipos cliente** en otras salas desde las que poder conectarse a los equipos de procesado de información centrales, los denominados hoy en día servidores. Con este hecho (el nacimiento de la **filosofía cliente-servidor**), el perímetro de seguridad se extendió y se incorporaron medidas de control de acceso de tipo «lógico», como complemento a las ya existentes medidas de control de acceso físico, para controlar el acceso a los sistemas desde ambos puntos de entrada. Un ejemplo de medida de control de acceso lógico es el uso de la dupla usuario y contraseña, que no es más que el traslado al mundo de la informática de protocolos tan añejos como el «santo y seña» militar.

Continuando con este breve viaje en el tiempo, en una etapa posterior, la evolución de la tecnología posibilitó la capacidad de **acceder a los sistemas de una organización** desde el exterior de la red de la empresa o red interna, es decir, acceder de forma remota a través de redes externas, como es internet, la conocida red de redes (que es una red pública), lo que implica que la seguridad perimetral ampliaba significativamente su ámbito de actuación. En esta disposición, que aún perdura, debemos preocuparnos especialmente de la «frontera» entre la **red interna** (es decir, la red conformada por los equipos de nuestro despacho) y la **red externa**, que en la mayoría de los casos se corresponderá unívocamente con internet, como red pública universal.

«Cloud Computing» Finalmente, se produjo otro cambio evolutivo que convive con los accesos remotos y los sistemas locales (un sistema local sería, por ejemplo, un servidor de ficheros en nuestro despacho). Se trata del *Cloud Computing* o computación en la **nube** (lo veremos con más detalle en el capítulo 10).

En este caso, es un **proveedor de servicios** (empresa tercera como puede ser Microsoft, Google, o Amazon, etc.) el que nos ofrece un servicio ya preparado para funcionar de manera inmediata o cuasi-inmediata. En otras palabras, nuestro servidor de ficheros ubicado y localizado física y tangiblemente en nuestras oficinas pasa a ser ubicuo y estar en las instalaciones de los citados proveedores. Mediante esta modalidad, nos conectamos al mismo a través de internet, y es el proveedor de servicios el encargado de tener diseñadas e implantadas instalaciones con medidas de seguridad físicas y proveer complementariamente ciertas medidas de seguridad lógicas, de acuerdo con el tipo de servicio prestado.

Otro ejemplo sencillo es el **correo electrónico** que nos puede prestar cualquiera de estos grandes proveedores, en el cual el proveedor se encarga a cambio de una cuota mensual de proveernos de un servicio final (el de correo electrónico para nuestra empresa con un cierto número de buzones o cuentas) a través de internet, sin que tengamos que disponer de un servidor local, ni preocuparnos de su configuración, de su mantenimiento, ni por ende de su seguridad.

Seguridad perimetral De forma adicional, el auge del empleo de arquitecturas enfocadas a la nube supuso que las medidas de control tradicionales para el control del perímetro, se tuviesen que adaptar o bien adoptar nuevas medidas para ese nuevo escenario donde los sistemas se administran por un proveedor de servicios y ya no están en nuestras instalaciones. Es por este motivo por el cual el perímetro se ha extendido, hasta convertirse en una nueva dimensión (a veces difusa y compleja de identificar en algunos casos), que es necesaria proteger, y para ello se siguen y apli-

can medidas y salvaguardas en el ámbito que se conoce como seguridad de red o seguridad perimetral.
Una **definición** academicista de seguridad perimetral podría ser la siguiente: la seguridad perimetral, en términos informáticos, se corresponde con la integración de elementos y sistemas emplazados en una arquitectura de red con el fin de proporcionar protección a las redes privadas frente amenazas, ataques y denegaciones de servicio provenientes de otras redes externas (como pueda ser internet).
Dado el ecosistema de nuestro despacho profesional, lo primero que se debe entender y plantear para poder implantar y/o mejorar nuestra seguridad perimetral son las siguientes **consideraciones**:
1. ¿Utilizo una arquitectura cliente-servidor local? Por ejemplo, un servidor para compartir ficheros o expedientes en nuestras instalaciones al que se conectan los profesionales para compartir documentos de trabajo.
2. ¿Utilizo servicios en la nube? Por ejemplo, un correo web, como gmail o hotmail, etc.
3. ¿Tengo servicios públicos en internet? Por ejemplo, extranet o repositorio documental a facturas o documentos con acceso privado para clientes.
4. Identificar qué servicios o actividades específicas dependen de cada modalidad.

Identificación de servicios Dado que usualmente se utiliza un híbrido de ambos tipos, es muy importante identificar como primer paso qué servicios se utilizan tanto en local como en la nube.
Es igualmente muy importante identificar todos los servicios puesto que cualquiera de ellos que pueda no estar controlado adecuadamente podría ser un **punto de fallo** de nuestra seguridad perimetral, como una pequeña fisura en un muro de hormigón de una presa.
a) ¿Qué servicios requieren y podría autorizar a que los usuarios (bien propios o terceros) se conecten desde fuera del despacho?
b) ¿Qué servicios no deben estar disponibles («publicarse» o ser visibles) desde internet?
Este será un primer punto de partida para a partir de aquí, **identificados nuestros servicios** y teniendo claro qué servicios son internos o externos plantear una política o directrices básicas que permitan comenzar a desplegar aquellas medidas de seguridad perimetral más adecuadas a nuestro negocio, según los posibles riesgos y necesidades.

3. Objetivos de la seguridad perimetral

Como se ha indicado, el principal objetivo de la seguridad perimetral es constituirse como la primera línea de defensa ante intentos de **acceso externos** a los sistemas de información de la organización.
Para alcanzar dicho objetivo, la seguridad perimetral se encarga de controlar las conexiones que se realizan a los servicios que utiliza la organización en su día a día, controlando al acceso a los recursos que se publiquen hacia el exterior, sean servicios:
– **públicos a cualquier usuario**, tales como la página web de nuestro despacho; o
– **restringidos**, como por ejemplo el acceso remoto desde casa a los equipos de los empleados o al servidor de ficheros.
En consecuencia, la seguridad perimetral se focaliza sobre unos **objetivos claros** y concisos al respecto de la protección de la red interna de la organización, entre los que destacan los siguientes:
a) **Permitir y/o rechazar conexiones** hacia los servicios publicados. Este es un objetivo clave, el primer paso como ya vimos en el apartado anterior es determinar qué servicios (correo, acceso remoto a los equipos de los trabajadores, etc.) vamos a querer publicar.
Como directriz general, la **filosofía y estrategias** han de ser **conservadoras** y deben publicarse aquellos servicios imprescindibles. De este modo, por ejemplo, si los

empleados pueden acceder fuera de la oficina al correo electrónico sin necesidad de conectarse a sus equipos de la oficina (donde estará habitualmente configurado su correo corporativo), es un riesgo innecesario habilitar un servicio de conexión remota virtual (**VPN**) a sus equipos. También se puede, por ejemplo, limitar las conexiones por su origen, de manera que algunos servicios solo estén disponibles cuando se accede desde, por ejemplo, las direcciones IP de la red (y los equipos) de otra delegación.
b) **Restringir el tráfico de red a un cierto tipo**. Como puede ser permitir únicamente el tráfico de red de correo electrónico. Es decir, configurar nuestros sistemas de red de manera que no permitan conversaciones de otros protocolos, como por ejemplo tráfico web o de telefonía IP.
c) **Restringir el tráfico de red entre equipos**, a aquellos necesarios. Por ejemplo, solo el personal del área de administración puede «ver» o conectarse a los servidores de contabilidad.
d) **Proporcionar un punto único de conexión con el exterior**. Idealmente nuestra red será más fácil de administrar y asegurar si concentramos todo el tráfico por una misma salida o conexión a internet (por ejemplo: línea única a internet de entrada/salida de varias delegaciones frente a líneas individuales en cada una).
e) **Gestionar el tráfico entre la red interna y la red externa**. Esto lo desarrollamos más adelante en este capítulo.

Funciones de garantía Para llevar a cabo todos y cada uno de los objetivos definidos, idealmente la seguridad perimetral debería, en la medida de lo posible, cumplir con diversas funciones que garanticen un óptimo control del perímetro interno:
1. **Resiliencia** (palabra que denota la capacidad de continuidad y resistencia). Tiene que ser capaz de soportar ataques desde el exterior, es decir, desde la red externa de la organización.
2. **Identificación**. Adicionalmente a la resistencia a dichos ataques, debe de ser capaz de identificar y alertar sobre ellos de la manera más precoz y efectiva posible.
3. **Cuarentena**. Debe de detectar el servicio atacado y aislarlo, si es posible, con el fin de evitar incidencias mayores que afecten al conjunto de la red interna.
4. **Filtros**. La capacidad de identificar el tráfico sospechoso proveniente del exterior, y en cualquier caso, restringir todo aquel encaminado a realizar acciones maliciosas en la red interna.

4. Riesgos y principales vectores de ataque

Como se ha visto, fruto de la evolución de los sistemas informáticos, la globalización y la necesidad de disponer de los recursos de información de las entidades disponibles en cualquier momento, hizo florecer la necesidad de conectar los sistemas de información a redes públicas tal como internet, pero requiriendo de las apropiadas medidas de seguridad para mantener la confidencialidad, disponibilidad e integridad de la información manejada, suponiendo un modelo muchísimo más amplio y complejo de seguridad perimetral.

Amenazas principales Actualmente, la seguridad perimetral debe de hacer frente a dos grandes tipos de amenazas principales según su intencionalidad:
1. El primer tipo de riesgo surge de la amenaza de posibles atacantes cuyo objetivo sea **infiltrarse en la red y sistemas internos** de una organización en concreto. En estos casos, la motivación puede ser obtener un lucro económico mediante la venta de información obtenida, como extorsión, fraude, tráfico de influencias, espionaje industrial o bien la propia venganza, desprestigio/ataque a la imagen o el reconocimiento de los logros por conseguirlo.
Es curioso subrayar que puede fácilmente darse el caso que el objetivo inicial del ataque no sea el despacho en sí, sino tal vez sea un ataque indirecto dirigido a alguno de los clientes, por ejemplo y que los atacantes busquen el eslabón más débil de la cadena para lograr su meta final, sea cual fuere. En cualquier caso, este tipo de ata-