MANUAL DEL CURSO

Manual de Ciberseguridad y seguridad informática

Amenazas, redes, dispositivos, entorno laboral, incidentes, nube y buenas prácticas



Lee este manual online, gratis y sin registro

academia-formacion.com/manual-curso-ciberseguridad/

Cuando termines, haz el examen y obtén tu certificado en academia-formacion.com

Índice

Toca un título para saltar directamente a esa parte del manual.

MÓDULO I **Introducción a la ciberseguridad** **3**

Unidad I. ¿Qué es la ciberseguridad? 3
Unidad II. Amenazas, vulnerabilidades y riesgos 4
Unidad III. Importancia de la seguridad informática en la sociedad actual 5
Unidad IV. Principales tipos de ataques cibernéticos 6
Unidad V. Legislación y normativas aplicables 8

MÓDULO II **Seguridad en redes** **10**

Unidad VI. Conceptos básicos de redes informáticas 10
Unidad VII. TCP/IP y sus principales vulnerabilidades 11
Unidad VIII. Cortafuegos, VPN y segmentación de redes 12
Unidad IX. Cifrado en tránsito: TLS, HTTPS y certificados 14
Unidad X. Buenas prácticas en la gestión de redes Wi-Fi 15

MÓDULO III **Protección de sistemas y dispositivos** **18**

Unidad XI. Actualización y parcheo de software 18
Unidad XII. Antivirus y herramientas anti-malware 19
Unidad XIII. Seguridad en dispositivos móviles 21
Unidad XIV. Control de acceso, contraseñas y autenticación multifactor 22
Unidad XV. Gestión de usuarios y privilegios 24

MÓDULO IV **Seguridad en el entorno laboral** **26**

Unidad XVI. Seguridad en el teletrabajo 26
Unidad XVII. Políticas de uso aceptable y concienciación del personal 27
Unidad XVIII. Gestión de dispositivos corporativos y BYOD 28
Unidad XIX. Protección contra la ingeniería social 30
Unidad XX. Evaluación de riesgos y planes de contingencia 31

MÓDULO V **Gestión de incidentes de seguridad** **34**

Unidad XXI. Qué hacer ante un incidente de ciberseguridad 34
Unidad XXII. Detección y respuesta 36
Unidad XXIII. Copias de seguridad y recuperación de datos 37
Unidad XXIV. Simulacros y pruebas de estrés 39
Unidad XXV. Reporte de incidentes y comunicación con las autoridades 40

MÓDULO VI **Seguridad en la nube y el comercio electrónico** 43

Unidad XXVI. Riesgos asociados al uso de servicios en la nube 43

Unidad XXVII. Cifrado de datos en la nube 44

Unidad XXVIII. Seguridad en aplicaciones web 46

Unidad XXIX. Seguridad en las transacciones electrónicas 47

Unidad XXX. Consideraciones legales y éticas 49

MÓDULO VII **Seguridad informática y gestión de la información** 51

Unidad XXXI. Ciberseguridad y seguridad informática: definiciones y diferencias 51

Unidad XXXII. Principios de la protección de datos: la tríada CIA 52

Unidad XXXIII. Normativa de protección de datos: RGPD y legislación española 53

Unidad XXXIV. Clasificación y protección de la información sensible 54

Unidad XXXV. Planificación de auditorías de seguridad de la información 56

MÓDULO VIII **Buenas prácticas y herramientas** 58

Unidad XXXVI. Configuración segura de navegadores y aplicaciones 58

Unidad XXXVII. Monitorización y registro de actividades 59

Unidad XXXVIII. Herramientas de ciberseguridad: código abierto y comerciales 61

Unidad XXXIX. Contraseñas seguras y gestores de contraseñas 62

Unidad XL. Consejos para una vida digital segura (personal y profesional) 64

REPASO **Datos clave para el examen del curso de Ciberseguridad y seguridad informática** 66

MÓDULO I

Introducción a la ciberseguridad

Este módulo es la puerta de entrada al curso. Verás qué es la ciberseguridad y qué pretende proteger, cómo se distinguen amenazas, vulnerabilidades y riesgos, por qué importa tanto en la sociedad actual, cuáles son los ataques más habituales y qué leyes y estándares se aplican.

UNIDAD I

¿Qué es la ciberseguridad?

1 Definición

La **ciberseguridad** es la práctica de proteger sistemas, redes y programas informáticos frente a ataques digitales. Esos ataques buscan acceder a información sensible, modificarla o destruirla, interrumpir la actividad de una empresa o extorsionar a los usuarios.

2 Objetivos: la tríada CIA

Toda medida de seguridad se apoya en tres objetivos básicos:

CONFIDENCIALIDAD

La información solo es accesible para las personas autorizadas.

INTEGRIDAD

Los datos son precisos y coherentes, y nadie los altera sin permiso.

DISPONIBILIDAD

La información y los recursos están accesibles para los usuarios autorizados cuando los necesitan.

! EJEMPLO

Si alguien lee tu historial médico sin permiso, falla la confidencialidad; si modifica un dato, falla la integridad; si un ataque deja el sistema caído y no puedes consultarlo, falla la disponibilidad. (Aviso añadido a este manual.)

3 Breve evolución histórica

- **Años 70 y 80:** nace la preocupación por la seguridad de los sistemas, se crean las primeras normas y aparecen los primeros virus.
- **Años 90:** con la expansión de Internet crecen los ciberataques y se desarrollan los antivirus y otras herramientas de protección.

- **Del 2000 a hoy:** la ciberseguridad pasa a ser una prioridad mundial por el aumento de los ataques dirigidos y la aparición de normativas internacionales como el GDPR (en España, RGPD).

4 Su papel en lo personal y lo profesional

- **A nivel personal:** protege tu privacidad y evita la suplantación de identidad, el robo de información y los fraudes en línea.
- **A nivel corporativo:** protege las operaciones, los datos de los clientes y los activos digitales. Exige políticas internas, formación del personal y medidas técnicas.

UNIDAD II

Amenazas, vulnerabilidades y riesgos

1 Tres conceptos que no son lo mismo

AMENAZA

Cualquier evento, acción o condición que podría aprovechar una vulnerabilidad y causar daño. Puede ser intencionada (un atacante) o accidental (un error humano, un desastre natural).

VULNERABILIDAD

Una debilidad de un sistema, red o proceso que una amenaza puede explotar. Puede ser técnica (un fallo del software) o humana (falta de formación).

RIESGO

La probabilidad de que una amenaza explote una vulnerabilidad, junto con la magnitud del daño que causaría.

El riesgo se expresa con una fórmula sencilla: **Riesgo = Probabilidad × Impacto**.

2 Ejemplos que los unen

Vulnerabilidad	Amenaza	Riesgo
Sistema operativo sin actualizar	Malware diseñado para aprovechar esa falta de actualización	Pérdida de datos o interrupción de servicios si el equipo se infecta
Web sin cifrado HTTPS que expone datos de tarjetas	Un atacante que busca datos bancarios	Que intercepte los datos, con impacto económico para los usuarios y para la reputación de la empresa

3 Clasificación de las amenazas

- **Humanas:** ataques de ciberdelincuentes, empleados desleales o errores accidentales. Por ejemplo, el phishing o la ingeniería social.

- **Tecnológicas:** problemas derivados del hardware o el software, como el malware o los ataques de denegación de servicio.
- **Naturales:** inundaciones, terremotos o incendios que dañan la infraestructura, por ejemplo los servidores.

4 Vulnerabilidades habituales

TÉCNICAS

- Software sin actualizar o sin parches.
- Contraseñas débiles.
- Puertos abiertos en redes mal configuradas.

HUMANAS

- Falta de formación en ciberseguridad.
- Caer en engaños de ingeniería social.
- Usar dispositivos personales en el trabajo sin protección.

5 Cómo se gestiona el riesgo

1. **Identificación:** detectar las amenazas potenciales y las vulnerabilidades del sistema.
2. **Análisis:** valorar la probabilidad de que ocurra un evento no deseado y su impacto.
3. **Tratamiento:** aplicar medidas para reducir el riesgo, como actualizar el software vulnerable o configurar cortafuegos que bloqueen accesos no autorizados.
4. **Seguimiento:** vigilar los sistemas de forma continua para detectar nuevas amenazas.

UNIDAD III

Importancia de la seguridad informática en la sociedad actual

1 Una sociedad que depende de lo digital

Gran parte de nuestra vida diaria, desde las operaciones bancarias hasta la comunicación o la educación, depende de la tecnología. Eso aporta enormes ventajas, pero también crea vulnerabilidades que los ciberataques pueden explotar. La seguridad informática es lo que mantiene este progreso estable y fiable.

2 Qué protege

INFORMACIÓN PERSONAL

Evita la suplantación de identidad, el robo de datos financieros o médicos y la invasión de la privacidad a través de dispositivos conectados.

INFRAESTRUCTURAS CRÍTICAS

Salud, energía, transporte y comunicaciones dependen de sistemas digitales. Un ataque podría interrumpir servicios esenciales, poner vidas en peligro y generar inestabilidad económica y social.

ECONOMÍA DIGITAL

Hace posible el comercio electrónico y la banca en línea, previniendo fraudes y pérdidas económicas y daños a la reputación.

3 Por qué cada vez importa más

- **Más ataques y más sofisticados,** contra personas y contra grandes organizaciones.
- **Cibercrimen organizado:** grupos especializados que se lucran con ransomware, phishing y otros métodos.
- **Riesgos geopolíticos:** los ciberataques pueden usarse como arma por estados o grupos organizados.
- **Internet de las cosas (IoT):** cuantos más objetos conectados hay, mayor es la superficie de ataque.

4 Beneficios de invertir en seguridad

- **Personas:** más privacidad y menos riesgo de fraude y de pérdida de datos.
- **Empresas:** continuidad de la actividad ante incidentes, cumplimiento legal sin sanciones y más confianza de clientes y socios.
- **Administraciones:** protección de los datos de la ciudadanía, resistencia ante ataques a infraestructuras críticas y prevención del espionaje.

5 Casos reales según el temario

- **2017, sistema sanitario del Reino Unido:** el ransomware WannaCry afectó a miles de ordenadores en hospitales, interrumpió servicios médicos y puso vidas en riesgo.
- **2021, red social:** se vieron comprometidas millones de cuentas, con exposición de datos personales y pérdida de confianza.

ATENCIÓN

Estos casos los recoge el temario sin más detalle; las cifras y las circunstancias exactas pueden haber cambiado o precisarse con el tiempo.

UNIDAD IV

Principales tipos de ataques cibernéticos

Un **ciberataque** es un intento malicioso de acceder a sistemas, redes o datos, alterarlos o destruirlos. Puede dirigirse a personas, empresas o gobiernos, y va desde simples engaños hasta operaciones muy sofisticadas. Estos son los ocho que recoge el temario.

Ataque	En qué consiste	Ejemplo	Cómo prevenirlo
Phishing	Engañar a una persona, con correos, mensajes o páginas falsificadas, para que entregue contraseñas, datos de tarjeta o datos bancarios.	Un correo falso de un banco que pide actualizar las credenciales.	Comprobar el remitente, no pulsar enlaces sospechosos y usar filtros antiphishing en el correo.
Malware	Software malicioso que daña, interrumpe o accede sin permiso a un sistema: virus, troyanos, gusanos, spyware.	Un adjunto infectado que instala un virus al abrirlo.	Mantener sistema y antivirus al día, descargar solo de fuentes fiables y analizar los equipos con regularidad.
Ransomware	Malware que cifra los datos y exige un pago para devolver el acceso.	WannaCry, que bloqueó datos de hospitales y empresas en 2017.	Copias de seguridad frecuentes, no abrir adjuntos ni enlaces desconocidos y aplicar las actualizaciones.
DoS y DDoS (denegación de servicio)	Sobrecargar un sistema o red con tráfico excesivo hasta dejarlo inoperativo. En el DDoS el tráfico llega desde muchos orígenes a la vez.	Una web inutilizada por millones de peticiones simultáneas.	Cortafuegos que filtren el tráfico malicioso y sistemas de vigilancia que detecten picos inusuales.
Ingeniería social	Manipulación psicológica para que las personas revelen información confidencial o hagan algo inseguro.	Alguien que se hace pasar por soporte técnico y pide acceso remoto al equipo.	Concienciar a la plantilla y fijar políticas de verificación de las solicitudes de acceso.
Fuerza bruta	Probar de forma automática muchísimas combinaciones de contraseñas hasta dar con la correcta.	Miles de intentos seguidos de entrar en una cuenta de correo.	Contraseñas complejas y únicas, bloqueo tras varios intentos fallidos y autenticación en dos pasos (2FA).
Inyección SQL	Aprovechar fallos de una aplicación web para introducir instrucciones no previstas en su base de datos y llegar a información sensible.	Obtener datos de clientes de una tienda en línea a través de su formulario de acceso.	Validar y filtrar lo que escriben los usuarios y usar consultas parametrizadas.
Ataques a dispositivos IoT	Dispositivos conectados, como cámaras o termostatos, que pueden ser vulnerables si carecen de medidas de seguridad.	Controlar a distancia una cámara de seguridad desprotegida.	Cambiar las contraseñas de fábrica y actualizar el firmware y el software.

1 Consecuencias

- **Personales:** robo de identidad, pérdida de privacidad y daños económicos.
- **Empresariales:** pérdida de datos, daño a la reputación y costes de recuperación.
- **Gubernamentales:** espionaje, sabotaje y afectación de infraestructuras críticas.

RECUERDA

Ninguna medida basta por sí sola: la prevención combina tecnología, buenas prácticas y concienciación constante. Cada uno de estos ataques se estudia con más detalle en los módulos siguientes.

UNIDAD V

Legislación y normativas aplicables

1 Para qué sirven

Las normas y estándares protegen la privacidad y los derechos de las personas, dan pautas claras para gestionar riesgos y proteger los datos, y ayudan a las organizaciones a cumplir los requisitos legales y evitar sanciones.

2 Principales marcos

GDPR / RGPD

Ámbito: Unión Europea, y también empresas de fuera que traten datos de ciudadanos europeos. **Objetivo:** proteger los datos personales y garantizar un tratamiento legal, transparente y seguro. **Claves según el temario:** derechos de acceso, rectificación, supresión («derecho al olvido») y portabilidad; obligación de notificar las brechas de seguridad en un máximo de 72 horas; multas de hasta el 4 % de la facturación global anual. **Ejemplo:** una empresa debe obtener consentimiento explícito antes de recopilar datos personales.

ISO 27001

Ámbito: estándar internacional de gestión de la seguridad de la información. **Objetivo:** establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja confidencialidad, integridad y disponibilidad. **Claves:** identificar y evaluar riesgos, aplicar controles y realizar auditorías periódicas. **Ejemplo:** una organización certificada demuestra a sus clientes que sigue buenas prácticas.

DSA (LEY DE SERVICIOS DIGITALES)

Ámbito: Unión Europea; regula plataformas en línea y redes sociales. **Objetivo:** más transparencia y seguridad en el entorno digital. **Claves:** retirada de contenido ilegal y protección de los derechos de los usuarios frente a abusos.

INFRAESTRUCTURAS CRÍTICAS

Ámbito: sectores clave como salud, transporte, energía y comunicaciones. **Objetivo:** proteger los servicios esenciales frente a las ciberamenazas.

NIST CYBERSECURITY FRAMEWORK

Ámbito: nacido en Estados Unidos, pero adoptado como referencia en todo el mundo.
Objetivo: un marco para identificar, proteger, detectar, responder y recuperarse ante ciberataques, con gestión continua del riesgo y válido para grandes y pequeñas empresas.

DATO ACTUALIZADO

El temario cita en algún punto la «LOPD», que ha quedado desfasada: hoy rigen el RGPD y la ley orgánica española que lo complementa. Plazos, importes y textos exactos pueden cambiar, así que comprueba siempre la normativa vigente en el BOE y en la AEPD. (Aviso añadido a este manual.)

3 Ventajas y desafíos del cumplimiento

VENTAJAS

- Protección legal: se evitan multas y sanciones.
- Reputación: más confianza de clientes, empleados y socios.
- Resiliencia: protocolos claros que reducen el impacto de los incidentes.

DESAFÍOS

- Cumplir varias normativas que pueden variar según el país o el sector.
- Seguir el ritmo de los cambios legales y tecnológicos.
- Integrarlas en los procesos sin perder productividad.

RECUERDA

La ciberseguridad protege la confidencialidad, la integridad y la disponibilidad de la información, y es responsabilidad de todos. Conocer amenazas, vulnerabilidades y riesgos, y cumplir la normativa, es la base para todo lo que viene después.

MÓDULO II

Seguridad en redes

Casi todo lo que haces con un dispositivo pasa por una red. En este módulo verás cómo funcionan las redes y el protocolo TCP/IP, qué debilidades tienen, con qué herramientas se protegen (cortafuegos, VPN y segmentación), cómo se cifra la información mientras viaja y cómo asegurar una red Wi-Fi.

UNIDAD VI

Conceptos básicos de redes informáticas

Una **red informática** es un conjunto de dispositivos interconectados que comparten recursos y datos. Es la base de Internet y de la actividad de empresas, administraciones y personas; por eso conviene conocer sus piezas antes de protegerlas.

1 Elementos de una red

DISPOSITIVOS FINALES

Los equipos con los que accedes a la red: ordenadores, móviles, tabletas, impresoras.

DISPOSITIVOS DE RED

Gestionan el tráfico de datos: routers, switches y puntos de acceso inalámbrico.

MEDIOS DE TRANSMISIÓN

Por cable (par trenzado, fibra óptica, coaxial) o inalámbricos (Wi-Fi, Bluetooth, ondas de radio).

PROTOCOLOS

Reglas que fijan cómo se comunican los dispositivos: TCP/IP, HTTP, FTP, DNS.

2 Tipos de red

Criterio	Tipo	Qué es
Alcance	LAN (red local)	Espacio reducido, como una oficina o una casa.
Alcance	MAN (red metropolitana)	Conecta redes dentro de una ciudad o región.
Alcance	WAN (red de área amplia)	Gran alcance; Internet es el ejemplo más conocido.
Diseño	Punto a punto (P2P)	Los dispositivos se comunican directamente entre sí.
Diseño	Cliente-servidor	Un servidor central gestiona la comunicación y los recursos compartidos.

3 Cómo viajan los datos

- **Paquetes:** los datos se dividen en paquetes que van del emisor al receptor por las rutas disponibles.
- **Direcciones IP:** identificadores únicos que localizan a cada dispositivo en la red.
- **Modelo OSI:** marco teórico que describe la transferencia en siete capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

Además, el rendimiento de una red depende de la **latencia** (retraso en la transferencia), el **ancho de banda** (capacidad máxima de transferencia) y, en redes inalámbricas, de las **interferencias** de otros dispositivos.

UNIDAD VII

TCP/IP y sus principales vulnerabilidades

TCP/IP (Transmission Control Protocol/Internet Protocol) es el conjunto de protocolos que permite que dispositivos de redes distintas se comuniquen, y es la base de Internet. Nació en los años 70 en el proyecto ARPANET y funciona con independencia del hardware y del sistema operativo.

1 Piezas del protocolo

IP

Direcciona y enruta los paquetes. IPv4 usa direcciones de 32 bits (por ejemplo, 192.168.1.1); IPv6, de 128 bits.

TCP

Orientado a conexión: divide los datos en paquetes, los reensambla en destino y reenvía los que se pierden, para una entrega fiable.

ASOCIADOS

HTTP/HTTPS (web), FTP (transferencia de archivos) y DNS (traduce nombres de dominio a direcciones IP).

2 Las cuatro capas del modelo TCP/IP

1. **Enlace de datos:** transmisión física a través del hardware.
2. **Internet:** direccionamiento y enrutamiento de paquetes.
3. **Transporte:** entrega correcta de los datos entre dispositivos.
4. **Aplicación:** interacción con los programas del usuario.

3 Vulnerabilidades y ataques habituales

TCP/IP se diseñó pensando en conectar, no en proteger. De ahí que existan estas amenazas (aquí solo se explica en qué consisten y cómo defenderse):

Amenaza	En qué consiste	Consecuencia
Suplantación de IP (IP spoofing)	Se falsifica la dirección IP para hacerse pasar por otro dispositivo.	Ataques DDoS o accesos no autorizados.
Man-in-the-Middle (MitM)	Alguien intercepta y puede manipular la comunicación entre dos dispositivos.	Robo de contraseñas o datos bancarios.
Escaneo de puertos	Se buscan puertos abiertos para localizar servicios vulnerables.	Facilita ataques posteriores a servicios inseguros.
Denegación de servicio (DoS/DDoS)	Se sobrecarga un servidor o una red hasta que deja de funcionar.	Paralización de servicios esenciales.
Manipulación de DNS (DNS spoofing)	Se alteran los registros DNS para redirigir el tráfico a sitios maliciosos.	Robo de credenciales y difusión de malware.

! CORREGIDO

El original habla de «fallas en DNS»; se ha reformulado como manipulación de los registros DNS, que es lo que describe el propio temario. (Aviso añadido a este manual.)

4 Cómo reducir el riesgo

- **Segmentar la red** para limitar accesos y contener incidentes.
- **Cifrar** la información en tránsito con HTTPS y VPN.
- **Mantener actualizados** sistemas, protocolos y dispositivos.
- **Monitorizar** con herramientas de detección de intrusos para identificar actividad sospechosa.
- **Configurar cortafuegos** y políticas de acceso que limiten el tráfico no autorizado y protejan los puertos.

UNIDAD VIII

Cortafuegos, VPN y segmentación de redes

Tres herramientas fundamentales para defender una red frente a amenazas externas e internas.

1 Cortafuegos (firewalls)

Un **cortafuegos** vigila y controla el tráfico entrante y saliente según reglas predefinidas. Actúa como barrera entre una red de confianza (la interna) y otra que no lo es (como Internet): bloquea lo no autorizado y deja pasar solo el tráfico legítimo.

Tipo	Cómo funciona
Filtrado de paquetes	Permite o bloquea según direcciones IP, puertos y protocolos.
Con estado (stateful inspection)	Además, recuerda el estado de las conexiones, lo que supera las limitaciones del filtrado simple.
De aplicación (proxy)	Filtra en la capa de aplicación (HTTP, FTP...) y puede bloquear aplicaciones maliciosas.
De próxima generación (NGFW)	Combina filtrado, inspección de estado y control avanzado de aplicaciones.

2 Redes privadas virtuales (VPN)

Una **VPN** crea una conexión cifrada a través de una red pública, de modo que el dispositivo se conecta a una red privada como si estuviera físicamente en ella. Sirve para proteger los datos en tránsito y para que el personal acceda de forma segura a los recursos de la empresa desde fuera.

- **VPN basada en SSL/TLS:** habitual en conexiones remotas y acceso a servicios web seguros.
- **VPN basada en IPsec:** más adecuada para unir redes entre sí.
- **VPN de acceso remoto:** permite que portátiles o móviles se conecten a la red interna.

! CORREGIDO

El original distingue «VPN de software (SSL/TLS)» y «de hardware (IPsec)». IPsec es un conjunto de protocolos, no un tipo de equipo, así que se clasifica por el protocolo. También se matiza que la VPN oculta tu IP ante los sitios que visitas, pero el proveedor de la VPN sí conoce tu tráfico. (Aviso añadido a este manual.)

3 Segmentación de redes

Consiste en **dividir una red en subredes más pequeñas**. Si un segmento se ve comprometido, la amenaza no se propaga al resto; además se controla mejor el acceso, se reduce el tráfico innecesario y es más fácil cumplir normativas de protección de datos como el RGPD.

VLAN

Redes lógicas separadas dentro de una misma red física, creadas con switches.

SUBREDES IP

División de la red con máscaras de subred.

ZONAS DE SEGURIDAD

Áreas con distintos niveles de acceso y control, separadas por cortafuegos o routers.

4 Buenas prácticas

- **Cortafuegos:** reglas específicas que permitan solo el tráfico necesario; revisarlas y consultar los registros (logs) con regularidad.
- **VPN:** cifrado robusto (como AES), autenticación multifactor y evitar servicios VPN gratuitos poco fiables.
- **Segmentación:** aislar los segmentos sensibles (información confidencial) y aplicar políticas de acceso estrictas según las necesidades de cada grupo.

UNIDAD IX

Cifrado en tránsito: TLS, HTTPS y certificados

El **cifrado en tránsito** protege los datos mientras viajan entre dispositivos. Aporta tres garantías: **confidencialidad** (solo el destinatario puede leerlos), **integridad** (no se alteran por el camino) y **autenticación** (se comprueba la identidad del servidor para evitar suplantaciones).

1 TLS

TLS (Transport Layer Security) es el protocolo criptográfico que asegura las comunicaciones en una red. Sustituyó a SSL, aunque aún se habla de «SSL» de forma coloquial. Su funcionamiento básico es:

1. **Handshake:** cliente (por ejemplo, un navegador) y servidor negocian una conexión segura.
2. **Intercambio de claves:** acuerdan las claves con las que cifrarán la comunicación.
3. **Cifrado:** a partir de ahí, todo lo que se envía va cifrado y un tercero no puede leerlo.
4. **Verificación de identidad:** el servidor presenta un certificado digital emitido por una autoridad de certificación (CA).

> **! CORREGIDO**
> El original dice que cliente y servidor «intercambian claves públicas y privadas». La clave privada nunca se comparte: solo se intercambia información pública para acordar las claves de sesión. (Aviso añadido a este manual.)

2 HTTPS

HTTPS es HTTP (el protocolo de la web) combinado con TLS. Con él, navegador y servidor hacen el handshake, los datos que envías (contraseñas, números de tarjeta...) viajan cifrados y el certificado confirma que el sitio es el legítimo. Protege frente a ataques MitM y es imprescindible en compras en línea, banca electrónica y cualquier envío de datos personales.

3 Certificados digitales y autoridades de certificación

- **Certificado digital:** archivo que contiene información sobre una organización y su clave pública; sirve para verificar la identidad de un sitio o servidor.

- **Autoridad de certificación (CA):** entidad de confianza que comprueba la identidad del titular antes de emitir el certificado.
- **Validación:** el navegador comprueba que el certificado sea válido, que lo haya emitido una CA fiable y que no esté revocado. Si falla algo, muestra una advertencia.

> **ATENCIÓN**
> Si el navegador te avisa de un certificado no válido, caducado o de origen dudoso, no continúes para introducir contraseñas o datos de pago. (Aviso añadido a este manual.)

4 Riesgos del cifrado en tránsito

Riesgo	Qué ocurre	Mitigación
Ataque de degradación (downgrade)	Se fuerza la conexión a una versión antigua y vulnerable de SSL/TLS.	Desactivar versiones antiguas y usar TLS 1.2 o 1.3.
Certificados falsos o CA comprometida	Se pueden interceptar y manipular las comunicaciones.	Verificar los certificados y usar solo certificados válidos de CA fiables.
Mala gestión de claves	Si se compromete la clave privada del servidor, el tráfico cifrado puede descifrarse.	Guardar las claves privadas en almacenamiento seguro y renovarlas con un ciclo adecuado.

> **CORREGIDO**
> El original llama «ataques de downgraded» a los ataques de degradación (downgrade) de versión. (Aviso añadido a este manual.)

5 Buenas prácticas para quien administra una web

- Usar HTTPS en todas las páginas, sobre todo en las que manejan datos sensibles.
- Contar con un certificado válido de una CA fiable y revisarlo periódicamente (caducidad, cadena de confianza, revocación).
- Forzar TLS 1.2 o 1.3 y deshabilitar protocolos obsoletos como SSL 2.0 y SSL 3.0.
- Activar HSTS (HTTP Strict Transport Security) para que el navegador exija siempre conexiones seguras.

UNIDAD X

Buenas prácticas en la gestión de redes Wi-Fi

El Wi-Fi da comodidad y movilidad, pero también expone a accesos no autorizados, interceptación de datos y ataques de denegación de servicio. Estas son las medidas esenciales.

1 Nombre de red (SSID)

El **SSID** es el nombre que identifica tu red Wi-Fi.

- Cambia el SSID de fábrica (muchos nombres delatan la marca y el modelo del router, lo que ayuda a un atacante).
- Elige un nombre que no revele datos de la red, como el nombre de la empresa o la ubicación.
- Ocultar el SSID es opcional: no es una medida de seguridad real, solo hace la red menos visible.

2 Cifrado Wi-Fi

Protocolo	Valoración
WPA3	El más reciente y robusto; resiste mejor los ataques de diccionario y la interceptación de datos.
WPA2	Alternativa aceptable si el router o los dispositivos no admiten WPA3.
WEP y WPA	Obsoletos, con vulnerabilidades conocidas: evítalos.

! CORREGIDO

El original presenta WPA2 como «el estándar más seguro disponible», lo que contradice que WPA3 sea el más robusto. Se ha reformulado como alternativa cuando WPA3 no está disponible. (Aviso añadido a este manual.)

3 Contraseña y autenticación

- Contraseña de al menos 12 caracteres, con mayúsculas, minúsculas, números y símbolos, sin palabras comunes ni secuencias simples como «123456».
- Cámbiala si sospechas de un acceso no autorizado y, si lo necesitas, guárdala en un gestor de contraseñas.
- En redes Wi-Fi de empresa, añade una segunda capa de verificación (autenticación multifactor) además de la contraseña.

4 Control de acceso y segmentación

- **Redes separadas** para empleados, invitados y dispositivos IoT: si un aparato IoT se ve comprometido, no afecta a la red principal.
- **Red de invitados** con salida a Internet pero sin acceso a recursos internos.
- **Filtrado de direcciones MAC:** limita el acceso a dispositivos concretos, pero las direcciones MAC pueden falsificarse, así que no debe ser la única medida.

5 Mantenimiento del router

- Actualiza el firmware: los fabricantes corrigen vulnerabilidades con cada versión. Activa la actualización automática o revísala de vez en cuando.
- Cambia la configuración por defecto, como contraseñas débiles de administración o la administración remota abierta.

! EJEMPLO

En casa, puedes dejar el ordenador y el móvil en la red principal y conectar la televisión, las bombillas inteligentes y las visitas a una red de invitados: si uno de esos aparatos se ve comprometido, tus datos personales quedan fuera de su alcance. (Aviso añadido a este manual.)

! RECUERDA

Una red segura combina varias capas: conocer cómo viaja el tráfico, filtrarlo con cortafuegos, segmentar, cifrar con TLS/HTTPS o VPN y mantener un Wi-Fi bien configurado (WPA3 o WPA2, contraseña robusta y router actualizado).

MÓDULO III

Protección de sistemas y dispositivos

Este módulo reúne las defensas básicas de cualquier equipo o cuenta: mantener el software al día, usar protección frente al malware, cuidar el móvil, controlar quién entra y con qué credenciales, y repartir los permisos con criterio. Son medidas sencillas, pero son las que más ataques evitan.

> **! AVISO**
>
> Los nombres de herramientas que aparecen son solo ejemplos para situarte. Los productos cambian, se renombran y desaparecen: compara siempre opciones actuales antes de elegir.

UNIDAD XI

Actualización y parcheo de software

1 Parche y actualización: qué son

Un **parche de seguridad** es una corrección que publica el fabricante para cerrar una vulnerabilidad, es decir, un fallo que un atacante podría aprovechar. Una **actualización** es un concepto más amplio: incluye parches, pero también mejoras de funciones, de rendimiento y corrección de errores que nada tienen que ver con la seguridad.

Mantener el software al día importa porque la mayoría de los ataques usan fallos *ya conocidos y ya corregidos*: quien no parchea sigue expuesto a un problema que tiene solución. Además, normas como ISO 27001 y el RGPD esperan que las organizaciones mantengan sus sistemas actualizados para proteger los datos personales.

2 Tipos de actualizaciones

SEGURIDAD

Corrigen vulnerabilidades (por ejemplo, fallos que permiten ejecutar código a distancia o elevar privilegios). Son la prioridad.

FUNCIONALIDAD

Añaden o mejoran funciones. Útiles, pero no deben pasar por delante de las de seguridad.

MANTENIMIENTO

Corrigen errores menores de funcionamiento sin impacto directo en la seguridad.

3 Ciclo del parcheo

1. **Detección:** fabricantes, equipos de seguridad e investigadores descubren la vulnerabilidad y la

clasifican por gravedad e impacto.

2. **Desarrollo:** el fabricante crea el parche, para una o varias versiones del software.
3. **Pruebas:** en un entorno de prueba se comprueba que el parche no rompe otras aplicaciones.
4. **Implantación:** se instala de forma automática, manual o con una herramienta de gestión de parches.
5. **Verificación:** se confirma que la vulnerabilidad está cerrada y que el sistema funciona con normalidad.

4 Cómo gestionar las actualizaciones

Método	Cómo funciona	Ventaja	Inconveniente
Actualización automática	El sistema o la aplicación descarga e instala los parches sin intervención.	Seguridad inmediata y sin olvidos.	Puede interferir con otras aplicaciones; en sistemas críticos se suele probar antes.
Gestión centralizada	Una herramienta controla desde un punto el parcheo de todos los equipos de la organización.	Todos los equipos al día y con trazabilidad.	Requiere montarla y mantenerla (ejemplos: WSUS, ManageEngine Patch Manager Plus).

5 Buenas prácticas

- Aplicar cuanto antes los parches de seguridad, empezando por los críticos.
- Mantener un **inventario** de programas y sistemas operativos: no se puede parchear lo que no se sabe que existe.
- Probar en un entorno de pruebas antes de pasar a producción.
- Automatizar siempre que sea posible.
- Vigilar de forma continua nuevas vulnerabilidades.

UNIDAD XII

Antivirus y herramientas anti-malware

1 Virus, malware y antivirus

Malware es cualquier software diseñado con fines maliciosos. El **virus** es solo un tipo concreto: se adjunta a archivos o programas legítimos y se propaga cuando se ejecutan. Un antivirus clásico se centra en virus; las herramientas anti-malware cubren un abanico más amplio de amenazas, y hoy la mayoría de productos combinan ambas funciones.

VIRUS

Infecta archivos y programas; puede corromperlos o destruirlos.

GUSANO (WORM)

Se copia a sí mismo y se propaga por redes sin necesitar un archivo anfitrión.

TROYANO

Se hace pasar por software legítimo para robar datos o dar acceso remoto al atacante.

RANSOMWARE

Cifra los archivos y exige un rescate. Suele llegar por correos de phishing, fallos sin parchear o webs comprometidas.

SPYWARE

Espía la actividad del usuario y roba información o credenciales.

ADWARE

Muestra anuncios no deseados; no suele destruir nada, pero ralentiza el equipo y afecta a la privacidad.

2 Cómo detectan las amenazas

Método	Qué hace	Ventaja	Limitación
Por firmas	Compara cada archivo con una base de datos de malware conocido.	Rápido y fiable con amenazas conocidas.	No detecta malware nuevo o desconocido.
Heurística	Analiza el código y busca rasgos sospechosos aunque no haya firma.	Puede detectar malware desconocido.	Falsos positivos con programas legítimos de aspecto sospechoso.
Por comportamiento	Observa en tiempo real lo que hace un programa (modificar archivos, acceder a datos personales).	Detecta amenazas sin firma conocida.	Consume más recursos y puede dar falsas alarmas.

Un buen producto actualiza a menudo sus datos de amenazas, protege en tiempo real, permite análisis programados y no ralentiza el equipo. Ejemplos: Microsoft Defender, Malwarebytes o Bitdefender.

3 Buenas prácticas de uso

1. **Mantén el antivirus actualizado**, tanto el programa como sus definiciones.
2. **Haz análisis completos periódicos**, aunque tengas protección en tiempo real.
3. **Instala solo software de fuentes fiables**: las descargas de sitios dudosos son una de las vías principales de infección.

4. **No lo desactives**: algunos malware intentan apagarlo, y desactivarlo «un momento» deja la puerta abierta.
5. **Añade más capas**: cortafuegos, filtrado de contenido y detección de intrusiones. Un antivirus solo no basta.

UNIDAD XIII

Seguridad en dispositivos móviles

1 Por qué el móvil es un objetivo

Un teléfono o una tableta guarda contraseñas, fotos, correo, aplicaciones bancarias y datos de trabajo. Sufre los riesgos de un ordenador (virus, phishing) y otros propios de su uso en movimiento:

- **Robo o pérdida:** da acceso directo a toda la información del dispositivo.
- **Malware móvil:** troyanos, ransomware o adware, normalmente por apps de fuentes no oficiales o enlaces inseguros.
- **Wi-Fi públicas:** alguien podría interceptar la comunicación entre tu móvil y el servidor (ataque «Man-in-the-Middle», MITM) y robar contraseñas o datos bancarios.
- **Phishing móvil:** mensajes engañosos por SMS (*smishing*) o mensajería instantánea para robar cuentas o instalar malware.
- **Apps maliciosas:** las tiendas oficiales filtran, pero alguna se cuela y puede espiar o robar datos.

2 Medidas de protección

- **Bloqueo de pantalla** con PIN, patrón o biometría.
- **Cifrado del dispositivo**, para que los datos sean ilegibles sin la clave si se pierde o roban.
- **Sistema y aplicaciones actualizados** (ver la Unidad 1).
- **Apps solo de tiendas oficiales**, revisando reseñas y permisos antes de instalar.
- **Antivirus para móvil** como protección adicional (análisis de apps, aviso de phishing).
- **Verificación en dos pasos** en correo, redes y banca (ver la Unidad 4).
- **Bluetooth y Wi-Fi apagados** cuando no se usan, sobre todo en sitios públicos.
- **VPN** (red privada virtual) si tienes que usar una Wi-Fi pública, y evita en ella operaciones sensibles.
- **Copias de seguridad** periódicas de fotos, contactos y documentos.

Ejemplos de herramientas: Google Play Protect (análisis de apps en Android) y las funciones de localización y bloqueo remoto de Apple y Google para dispositivos perdidos o robados.

3 Móviles en la empresa

Si el empleado accede a información confidencial desde su móvil, el riesgo se multiplica. Estrategias clave:

- **MDM (gestión de dispositivos móviles):** controla el acceso a sistemas corporativos, impone políticas (por ejemplo, requisitos de contraseña) y permite borrar datos a distancia si el dispositivo se pierde.
- **Aplicaciones corporativas aprobadas** y actualizadas.
- **VPN** obligatoria para acceder a la red de la empresa y proteger los datos en tránsito.

UNIDAD XIV

Control de acceso, contraseñas y autenticación multifactor

1 Control de acceso y métodos de autenticación

El **control de acceso** decide quién puede entrar a un sistema, red o recurso, para evitar robos de datos, cambios no autorizados o ataques. Se apoya en el principio de **«necesidad de saber»**: cada persona accede solo a lo que necesita para su trabajo. La **autenticación** es la comprobación de que quien intenta entrar es quien dice ser.

CONTRASEÑA

El método más común. Es vulnerable si es fácil de adivinar, se reutiliza o se filtra.

TARJETA O TOKEN

Dispositivo físico que genera códigos únicos o actúa como llave. No depende solo de la contraseña.

BIOMETRÍA

Huella, rostro o iris. Habitual en móviles y sistemas de alta seguridad.

COMPORTAMIENTO

Analiza cómo escribes, mueves el ratón o accedes. Se usa como capa adicional.

2 Contraseñas seguras

Las contraseñas débiles (fechas de nacimiento, «123456») caen ante ataques de fuerza bruta (probar combinaciones masivamente) y de ingeniería social. Para crear una buena:

- **Longitud:** al menos 12 caracteres; cuanto más larga, más difícil de descifrar.
- **Variedad:** mayúsculas, minúsculas, números y símbolos.
- **Nada previsible:** evita palabras de diccionario, nombres propios, fechas o datos personales como mascotas y ciudades.
- **Frases de paso (*passphrases*):** varias palabras sin relación entre sí son largas, fáciles de recordar y mucho más sólidas que una contraseña corta.
- **Una distinta para cada cuenta**, para que la filtración de una no abra las demás.

CORREGIDO

El original propone como ejemplo «MiC0ntr@señ@d3Seguridad1». Sustituir letras por números y símbolos de forma típica (a por @, o por 0) es un patrón muy conocido que los atacantes ya prueban, así que no es un buen modelo. Se recomienda una frase larga de palabras sin relación. (Aviso añadido a este manual.)

DATO ACTUALIZADO

El temario recomienda cambiar las contraseñas con regularidad, pero advierte de que hacerlo con demasiada frecuencia lleva a elegir claves más simples. Las recomendaciones actuales de muchos organismos son cambiarlas cuando haya sospecha de que se han visto comprometidas y no por calendario; comprueba la política que aplique a tu caso. (Aviso añadido a este manual.)

Para no tener que memorizarlas todas, usa un **gestor de contraseñas** (ejemplos: Bitwarden, 1Password), que las guarda cifradas y genera claves complejas. Un servicio como *Have I Been Pwned* permite comprobar si tu correo aparece en una filtración de datos; si es así, cambia las contraseñas afectadas.

3 Autenticación multifactor (MFA)

La **MFA** exige al menos dos pruebas de categorías distintas. Así, aunque un atacante consiga tu contraseña, todavía debe superar otro factor.

Factor	Qué es	Ejemplos
Algo que sabes	Información que solo conoces. Es el factor más común y el más débil si va solo.	Contraseña, PIN, pregunta de seguridad.
Algo que tienes	Un objeto físico en tu poder.	Token de hardware, tarjeta, móvil que recibe un código.
Algo que eres	Un rasgo biológico tuyo.	Huella, rostro, iris.

EJEMPLO

Entras en tu correo: primero escribes la contraseña (algo que sabes), después abres tu aplicación de autenticación y escribes el código que muestra en ese momento (algo que tienes). Sin ambos pasos no se accede. (Aviso añadido a este manual.)

4 Métodos habituales de MFA

- **Aplicaciones de autenticación (OTP):** generan códigos de un solo uso que cambian cada 30 segundos (ejemplos: Google Authenticator, Authy, Microsoft Authenticator).
- **SMS:** cómodo, pero más vulnerable a ataques como el *SIM swapping* (el atacante consigue una tarjeta SIM duplicada con tu número).
- **Biometría:** añade una capa extra en móviles, aunque no es infalible.

VENTAJAS

Eleva mucho la seguridad de cuentas y sistemas, protege frente al robo de contraseñas y al phishing, y permite elegir método.

INCONVENIENTES

Es algo más lento, algunos métodos (SMS, tokens) tienen sus propias debilidades y no todos los servicios la ofrecen.

UNIDAD XV

Gestión de usuarios y privilegios

1 Tipos de usuarios

Gestionar usuarios y privilegios consiste en que cada persona acceda solo a los datos y herramientas que necesita. Los sistemas suelen distinguir cuatro tipos de cuenta:

ESTÁNDAR

Permisos básicos: usar aplicaciones y leer archivos. No puede cambiar la configuración del sistema.

ADMINISTRADOR

Control total: instala software, gestiona usuarios y cambia configuraciones críticas. Solo para personas de confianza.

INVITADO

Cuenta temporal con permisos muy limitados, sin acceso a información sensible.

DE SERVICIO

La usa una aplicación o un proceso automático, no una persona. Con permisos limitados a su tarea y bien protegida.

2 Principios de gestión de privilegios

- **Mínimo privilegio:** cada usuario tiene el acceso mínimo imprescindible; así se reducen errores y filtraciones.
- **Separación de funciones:** las tareas críticas se reparten entre personas. Por ejemplo, quien aprueba un pago no debería ser quien lo ejecuta, lo que dificulta el fraude.
- **Control de acceso basado en roles (RBAC):** los usuarios se agrupan en roles con permisos predefinidos; al asignar un rol se asignan sus permisos. Simplifica la gestión a gran escala y reduce errores.
- **Auditoría y monitorización:** registros (logs) de accesos y cambios de privilegios, alertas ante accesos fallidos y revisiones periódicas, sobre todo de los administradores.

3 Ciclo de vida de las cuentas

1. **Alta documentada:** registra quién crea la cuenta, qué privilegios recibe y para qué.
2. **Revisión periódica:** desactiva o elimina las cuentas inactivas o innecesarias.

3. **Cambios de puesto:** si alguien cambia de función, ajusta sus privilegios a la nueva.
4. **Baja inmediata:** al salir un empleado o colaborador externo, desactiva su cuenta de inmediato.

4 Herramientas

- **LDAP:** protocolo para almacenar y consultar información de usuarios en un directorio, que centraliza su gestión.
- **Active Directory:** servicio de directorio de Microsoft para gestionar usuarios, equipos y permisos por roles en una red.
- **IAM (gestión de identidades y accesos):** controla todo el ciclo de vida de las cuentas, aplica políticas y monitoriza accesos.
- **MFA** en las cuentas con privilegios elevados, que son las más codiciadas.

! RECUERDA

Mantén todo actualizado, protégete con antivirus y MFA, usa contraseñas largas y distintas, y da a cada usuario solo los permisos que necesita. Ninguna de estas capas basta por sí sola; juntas dificultan mucho el trabajo al atacante.

MÓDULO IV

Seguridad en el entorno laboral

La seguridad de una empresa no depende solo de la tecnología: también depende de dónde trabajan las personas, con qué dispositivos lo hacen y de lo bien que saben detectar un engaño. Este módulo repasa el teletrabajo seguro, las normas internas de uso, la gestión de dispositivos corporativos y personales, la ingeniería social y la preparación ante incidentes.

UNIDAD XVI

Seguridad en el teletrabajo

Al trabajar fuera de la oficina se pierde la red protegida de la empresa y aumentan los riesgos. Por eso el teletrabajo exige medidas propias, tanto del trabajador como de la organización.

1 Principales riesgos

- Conexiones de red poco seguras, como el Wi-Fi público de una cafetería o un aeropuerto.
- Acceso no autorizado a los dispositivos y sistemas de la empresa.
- Dispositivos personales vulnerables que se usan para tareas laborales.
- Fuga de información por un manejo incorrecto de los datos.

2 Buenas prácticas

RED SEGURA Y VPN

Conéctate a redes Wi-Fi protegidas con contraseña fuerte y cifrado. En casa, usa un cifrado robusto como WPA3 (si tu router lo admite). Si tienes que usar una red pública o poco fiable, activa una **VPN** (red privada virtual): cifra todo el tráfico entre tu dispositivo y la red de la empresa y dificulta que alguien lo intercepte.

DISPOSITIVOS PROTEGIDOS

Contraseñas seguras y MFA, sistema operativo y aplicaciones siempre actualizados (los parches corrigen vulnerabilidades conocidas) y antivirus instalado para frenar malware y programas espía.

MFA

La autenticación multifactor pide dos o más pruebas de identidad: además de la contraseña, un código por SMS o generado por una aplicación. Si te roban la contraseña, el acceso sigue protegido.

CONTRASEÑAS

Usa contraseñas únicas y largas (al menos 12 caracteres, con letras, números y símbolos) y un gestor de contraseñas para generarlas y guardarlas. Los datos sensibles deben almacenarse cifrados y con acceso restringido.

FORMACIÓN FRENTE AL PHISHING

El correo fraudulento es uno de los ataques más comunes en remoto. Verifica la autenticidad de un mensaje antes de pulsar un enlace o abrir un adjunto.

HERRAMIENTAS DE COLABORACIÓN

En videoconferencias, protege la reunión con contraseña, usa sala de espera para controlar quién entra y no publiques el enlace. En la nube, deja el acceso solo a las personas autorizadas, gestiona bien los permisos y activa el cifrado de archivos.

COPIAS Y RECUPERACIÓN

Haz copias periódicas de los documentos importantes, en la nube o en dispositivos externos cifrados, y que la empresa tenga un plan para restaurar sistemas e información.

3 Cumplimiento legal y respuesta ante incidentes

El teletrabajo debe respetar la normativa de protección de datos; en la Unión Europea, el Reglamento General de Protección de Datos (RGPD, GDPR en inglés), que obliga a proteger los datos personales también cuando se tratan desde casa.

Si detectas una brecha de seguridad, actúa así:

1. **Notifica de inmediato** el incidente al departamento de seguridad de la información.
2. **Contén y mitiga**: aísla lo afectado cuanto antes para que no se propague y reducir el daño.

UNIDAD XVII

Políticas de uso aceptable y concienciación del personal

Una **política de uso aceptable** (AUP, por sus siglas en inglés) es el conjunto de reglas que fija cómo pueden usar los empleados los recursos tecnológicos de la empresa de forma segura y responsable. Debe ser clara, comprensible y concreta; si nadie la entiende, nadie la cumple.

1 Qué debe incluir una AUP

Apartado	Qué recoge
Recursos permitidos	Qué equipos, redes, correo y herramientas se pueden usar; software autorizado (prohibiendo instalar el no verificado) y límites de uso de internet y redes sociales en horario laboral, bloqueando sitios peligrosos.
Dispositivos móviles	Cómo proteger smartphones y tablets que acceden a sistemas corporativos (contraseña fuerte, MFA, cifrado) y prohibición de guardar en ellos información sensible de la empresa, como credenciales o documentos confidenciales.

Apartado	Qué recoge
Contraseñas y autenticación	Longitud mínima (por ejemplo, 12 caracteres), combinación de tipos de carácter, no repetir contraseñas entre servicios y MFA obligatoria en sistemas críticos.
Privacidad y datos	Acceso solo a lo necesario para el trabajo (principio de mínimo privilegio), reglas para almacenar y transmitir datos y prohibición de compartir información confidencial sin autorización.
Actividades prohibidas	Actividades ilegales o no autorizadas: software pirata, acceso no autorizado a sistemas, uso de herramientas de ataque o escaneo, acoso, difamación o contenido inapropiado.
Sanciones	Consecuencias del incumplimiento, desde medidas disciplinarias hasta el despido en incidentes graves, con un proceso claro, imparcial y respetuoso con los derechos del trabajador.

2 Concienciación del personal

Las normas por sí solas no bastan: hace falta una **cultura de seguridad** en la que cada empleado se sienta parte de la defensa y anime a sus compañeros a seguir las buenas prácticas.

- **Formación continua y adaptada**: talleres sobre amenazas actuales (phishing, ransomware), contraseñas, correos fraudulentos y protección de móviles y redes.
- **Simulacros de phishing** periódicos para medir cómo reacciona la plantilla y enseñar a prevenirlos.
- **Comunicación accesible**: resúmenes visuales, infografías o vídeos en lugar de documentos largos y técnicos, y recordatorios regulares sobre nuevas amenazas.
- **Evaluación y mejora continua**: auditorías periódicas para comprobar que las políticas funcionan y siguen alineadas con las amenazas emergentes.

UNIDAD XVIII

Gestión de dispositivos corporativos y BYOD

Muchas empresas permiten usar dispositivos personales para trabajar. Eso aporta flexibilidad, pero obliga a distinguir bien entre los equipos de la empresa y los de los empleados.

1 Corporativo frente a BYOD

DISPOSITIVO CORPORATIVO

Lo proporciona la empresa (portátiles, móviles, tablets). Esta controla su configuración, mantenimiento y actualización.

BYOD (BRING YOUR OWN DEVICE)

El empleado usa su propio móvil, tablet u ordenador para acceder a los recursos de la empresa. El control de la organización es mucho más limitado.

2 Riesgos del BYOD

- **Acceso no autorizado** si el dispositivo se pierde o lo roban, porque suele tener menos controles.
- **Falta de cifrado**, que deja los datos expuestos en el equipo y en redes inseguras.
- **Malware y aplicaciones inseguras** instaladas por el usuario, que pueden infectar la red corporativa.
- **Control limitado** sobre aplicaciones y ajustes, lo que dificulta aplicar políticas uniformes.

3 Medidas de seguridad

Dispositivos corporativos

- Cifrado de todo el equipo, por si se pierde o se roba.
- Actualizaciones y parches automáticos.
- MFA obligatoria para acceder a equipos y sistemas.
- Control de acceso con mínimo privilegio.
- Gestión remota que permita borrar los datos si el dispositivo desaparece.

Dispositivos personales (BYOD)

- **Registro** del dispositivo en un sistema de gestión de móviles (MDM) para poder supervisar su seguridad.
- **Cifrado obligatorio** de los datos almacenados y de los que viajan por la red.
- **Separación** de datos personales y corporativos mediante contenedores seguros o espacios de trabajo virtuales.
- **Aplicaciones autorizadas**: lista de apps aprobadas y bloqueo del resto.
- **Políticas aplicadas con MDM**: exigir contraseñas seguras, bloquear ciertos servicios y gestionar el acceso a las apps corporativas.

4 Ventajas y desventajas del BYOD

Aspecto	Ventajas	Desventajas
Productividad	Se trabaja desde cualquier lugar y con el dispositivo preferido.	Los equipos personales suelen estar menos protegidos y aumenta el riesgo de brechas.
Coste y gestión	La empresa ahorra en hardware.	Gestionar una gran variedad de dispositivos es complejo y costoso.
Personas	Mayor satisfacción y motivación del empleado.	Cuesta separar lo personal de lo profesional, con riesgo para la privacidad de ambos.

5 Herramientas de gestión

- **MDM** (Mobile Device Management): administra y controla dispositivos móviles, corporativos o personales, con políticas centralizadas.

- **EMM** (Enterprise Mobility Management): solución más amplia que, además de los dispositivos, gestiona aplicaciones y datos.
- **VPN y cifrado**: protegen las comunicaciones y los datos en los móviles.

Las herramientas concretas del mercado cambian a menudo: fíjate en la función de cada categoría.

UNIDAD XIX

Protección contra la ingeniería social

La **ingeniería social** consiste en manipular psicológicamente a las personas para que realicen acciones o revelen información confidencial sin darse cuenta del engaño. No explota fallos técnicos, sino la confianza y el comportamiento humano, y por eso es tan eficaz.

1 Tipos habituales

PHISHING

Mensaje, normalmente un correo, que aparenta venir de una fuente fiable (un banco, un organismo público) y pide pulsar un enlace o abrir un adjunto para robar contraseñas, datos de tarjeta o credenciales.

SPEAR PHISHING

Versión dirigida: el mensaje se personaliza para una persona o grupo concreto, tras reunir información sobre la víctima.

VISHING

Phishing por llamada telefónica: el atacante se hace pasar por un banco o un proveedor para sacar información sensible.

BAITING (CEBO)

Se ofrece algo atractivo, como software o música gratis, para que la víctima descargue un archivo o pulse un enlace que instala malware o entrega datos.

PRETEXTING

El atacante inventa un escenario falso (por ejemplo, soporte técnico o investigador) para conseguir credenciales o datos de cuentas.

ENCUESTAS Y QUIZZES FALSOS

Pruebas de personalidad o encuestas aparentemente inofensivas que recopilan datos personales útiles para otros ataques.

2 Señales de alerta

- **Urgencia o amenazas**: «su cuenta ha sido comprometida, actúe ya para evitar el bloqueo».
- **Petición de datos sensibles** por correo, teléfono o SMS no solicitados: ninguna entidad legítima debería hacerlo.
- **Incongruencias**: faltas, enlaces que no coinciden con la web oficial o remitentes con direcciones casi idénticas a las reales.
- **Adjuntos o enlaces desconocidos** que pueden contener malware.

3 Cómo protegerse

- **Formación continua** con ejemplos reales de mensajes fraudulentos y protocolos de actuación.
- **Verificar la identidad** de quien pide algo sensible por otro canal oficial, como el teléfono oficial de la empresa.
- **No abrir enlaces ni archivos** de origen dudoso.
- **MFA y contraseñas únicas** en las cuentas importantes, para que un robo de credenciales no baste.
- **Cuidar lo que publicas** en redes sociales, porque los atacantes lo usan para personalizar sus engaños.
- **Control de acceso** para limitar el daño si una cuenta se ve comprometida.

Como apoyo técnico existen filtros avanzados de correo, antivirus y antimalware, soluciones de MFA y simuladores de phishing para entrenar a la plantilla.

4 Qué hacer si has caído

1. **Informa** de inmediato a TI o a seguridad para investigar y limitar el daño.
2. **Cambia las contraseñas** que puedan estar comprometidas y activa MFA si no la tenías.
3. **Revisa los sistemas** afectados para detectar accesos o malware (lo hace el equipo de TI).
4. **Documenta el incidente** para aprender de él y mejorar las políticas.

UNIDAD XX

Evaluación de riesgos y planes de contingencia

La **evaluación de riesgos** es el proceso sistemático con el que una organización identifica, analiza y valora los riesgos que pueden afectar a sus activos, datos y operaciones. Sirve para dirigir los recursos hacia las amenazas más críticas. No es algo que se haga una sola vez: los riesgos cambian y hay que revisarlos con regularidad.

1 Fases de la evaluación

1. **Identificar** los riesgos posibles, externos (ciberataques) o internos (errores humanos, fallos técnicos), sean tecnológicos, operativos, legales o financieros.
2. **Analizar** cada riesgo: cómo podría ocurrir, su probabilidad y la gravedad de sus consecuencias.
3. **Evaluar** cuáles son los más críticos, por ejemplo con una **matriz de riesgos** que los clasifique según probabilidad e impacto. Los de alta probabilidad y alto impacto van primero.
4. **Priorizar** según la urgencia, centrando los esfuerzos en los que causarían más daño o es más probable que ocurran.

2 Riesgos habituales en el entorno laboral

Riesgo	Consecuencia
Ciberataques (phishing, malware, ransomware)	Comprometen información crítica, dañan sistemas o paralizan la actividad.
Pérdida de datos o brechas	Pérdida de confianza de los clientes y posibles sanciones legales.
Errores humanos	Abrir correos maliciosos o revelar información sin querer.
Fallos tecnológicos y caídas	Servidores caídos o falta de conectividad que detienen las operaciones.
Desastres naturales o imprevistos	Inundaciones o incendios que dañan la infraestructura física.

3 Plan de contingencia

Un **plan de contingencia** es el conjunto de procedimientos que una organización pone en marcha para mantener su actividad cuando ocurre un suceso adverso. Su objetivo es minimizar el impacto y recuperarse lo antes posible, y debe estar alineado con las políticas de seguridad.

ACTIVOS CRÍTICOS

Identificar qué sistemas, aplicaciones y datos son esenciales y protegerlos de forma especial.

RESPUESTA A INCIDENTES

Qué hacer nada más ocurrir: avisar al personal, desconectar los sistemas comprometidos y activar las medidas de seguridad.

RECUPERACIÓN DE DATOS

Copias de seguridad y procedimientos de restauración para la información esencial.

COMUNICACIÓN

Protocolo claro, preciso y rápido para informar a empleados, clientes y otras partes interesadas.

RECUPERACIÓN DE OPERACIONES

Pasos para volver a la normalidad: reactivar sistemas, reubicar personal o usar infraestructuras alternativas.

PRUEBAS Y SIMULACROS

Ensayos periódicos para comprobar que el plan funciona y entrenar al personal.

4 Gestión de crisis y continuidad del negocio

En una crisis, la dirección debe coordinar los esfuerzos para reducir el impacto. El **plan de continuidad del negocio** (BCP, en inglés) amplía el plan de contingencia para que la organización siga operando durante y después de un evento disruptivo. Incluye:

- Evaluar la capacidad de respuesta ante crisis.

- Duplicar (redundancia) los sistemas críticos.
- Acordar la recuperación con proveedores y socios.
- Revisar y ajustar el plan continuamente según cambien la infraestructura, la tecnología, los procesos y las amenazas.

RECUERDA

La mayoría de los incidentes empiezan por una persona engañada o un dispositivo descuidado: combina normas claras, formación continua y un plan de contingencia probado.

MÓDULO V

Gestión de incidentes de seguridad

Ningún sistema es invulnerable, así que la pregunta no es solo cómo evitar un incidente, sino qué hacer cuando ocurra. Este módulo explica cómo responder con orden, cómo detectar a tiempo, cómo recuperar los datos con copias de seguridad, cómo entrenarse con simulacros y a quién hay que avisar y cuándo.

> **! AVISO**
>
> Las referencias legales (RGPD, LSSI-CE) y los plazos que aparecen proceden del temario y pueden cambiar. Antes de aplicarlos en una organización real, comprueba la normativa vigente en el BOE y en la web de la AEPD. (Aviso añadido a este manual.)

UNIDAD XXI

Qué hacer ante un incidente de ciberseguridad

1 Qué es un incidente

Un **incidente de ciberseguridad** es cualquier evento que compromete la **confidencialidad, la integridad o la disponibilidad** de los activos informáticos, los datos o los servicios de una organización. Su gravedad es muy variable: desde un error de configuración hasta un ataque que paraliza toda la infraestructura.

Los más habituales son el malware, el ransomware, el phishing, las brechas de datos, la denegación de servicio (DDoS) y los accesos no autorizados.

2 Las fases de la respuesta

Responder con improvisación suele empeorar el daño. Por eso la gestión de incidentes sigue un proceso por fases:

1. **Detección y confirmación.** Se identifica que algo anómalo está pasando (por monitorización, alertas del software de seguridad o avisos de los empleados) y se comprueba si es un incidente real o un *falso positivo*, es decir, una alerta que no indica un problema verdadero.
2. **Contención.** Se frena la propagación para limitar el daño: desconectar de la red los sistemas afectados, desactivar las cuentas comprometidas y bloquear el tráfico malicioso con reglas de cortafuegos.
3. **Erradicación.** Se elimina la causa raíz: borrar el malware, corregir la vulnerabilidad explotada, aplicar parches y revisar que no queden restos del ataque.
4. **Recuperación.** Se devuelven los sistemas y los datos a su estado normal, restaurando desde copias fiables, comprobando que todo es seguro antes de reconectarlo y manteniendo vigilancia

para detectar nuevos problemas.

5 **Lecciones aprendidas.** Se revisa lo ocurrido: cómo entró el atacante, qué falló y qué se puede mejorar. Con ello se actualizan planes, políticas y formación del personal.

! RECUERDA

El orden importa: primero contener, luego erradicar y solo después recuperar. Si restauras sistemas antes de eliminar la causa, el incidente puede repetirse.

3 Quién hace qué

Antes de que ocurra nada, cada persona debe saber cuál es su papel.

EQUIPO DE RESPUESTA (IRT)

Formado por personal de TI, seguridad, legal y comunicaciones. Coordina la respuesta y vela por que se sigan los procedimientos.

TI Y SEGURIDAD

Identifican y contienen el incidente, erradican la amenaza, restauran los sistemas y hacen el análisis forense.

LEGAL Y CUMPLIMIENTO

Comprueban que se cumple la normativa (por ejemplo, la notificación a las autoridades si se filtran datos personales) y que la evidencia se gestiona bien.

COMUNICACIÓN

Gestiona los avisos internos y externos para informar a empleados, clientes y otras partes interesadas con transparencia y profesionalidad.

4 Documentar todo, en el momento

Cada acción debe registrarse mientras ocurre. Ese registro sirve para recuperar, para evaluar después lo sucedido y, si hace falta, para posibles procedimientos legales. Debe incluir:

- Los datos del incidente: fecha, hora, impacto.
- Las decisiones tomadas durante la respuesta.
- Los recursos utilizados (herramientas, equipos).
- El resultado de cada fase.

Si el incidente implica actividad ilegal, como el robo de datos, la **evidencia digital** debe preservarse con cuidado para que pueda utilizarse más adelante.

5 Herramientas de apoyo

Los **SIEM** (gestión de eventos e información de seguridad) recogen y correlacionan eventos para detectar incidentes casi en tiempo real; las herramientas forenses conservan la evidencia; y los canales de comunicación seguros permiten coordinar la respuesta sin que el atacante lea lo que se dice.

CORREGIDO

El original llama «Sistemas de Gestión de Incidentes de Seguridad» a los SIEM. Las siglas corresponden a «Gestión de Eventos e Información de Seguridad» (Security Information and Event Management), nombre que se usa en la unidad siguiente. (Aviso añadido a este manual.)

UNIDAD XXII

Detección y respuesta

Cuanto antes se detecta un incidente, menos daño causa y menos tiempo permanece parada la actividad. La detección consiste en identificar comportamientos, patrones o actividades anómalas que indican que un ataque está en marcha o ya ha ocurrido.

1 Cómo se detecta

MONITORIZACIÓN CONTINUA

Vigilancia permanente de redes y sistemas con SIEM, con sistemas de detección y prevención de intrusiones (IDS/IPS) y con software de monitorización de red que revela picos de tráfico o comunicaciones sospechosas.

ANÁLISIS DE LOGS

Los registros de eventos de los sistemas cuentan qué ha pasado en la infraestructura. Hay que revisarlos con regularidad para localizar comportamientos inusuales.

ANÁLISIS DE COMPORTAMIENTO (UBA)

Detecta acciones raras de usuarios: accesos a horas extrañas, intentos de entrar en sistemas no autorizados o transferencias de grandes cantidades de datos.

La diferencia entre IDS e IPS es que el primero **detecta** y avisa, mientras que el segundo además puede **bloquear** la actividad sospechosa.

2 Clasificar y priorizar

Una vez detectado, el incidente se clasifica según su gravedad para decidir cuánta urgencia y cuántos recursos merece.

Tipo	Qué es	Ejemplo
Crítico	Afecta gravemente a la disponibilidad, integridad o confidencialidad de datos o sistemas.	Ransomware que cifra toda la infraestructura o una filtración masiva de datos.
Menos crítico	Riesgo menor y fácil de aislar.	Malware en un solo equipo que se puede aislar sin afectar al resto de la red.

Para priorizar se tienen en cuenta la probabilidad de impacto, el daño potencial, el coste asociado y el tiempo de inactividad que podría provocar.

3 Responder y apoyarse en herramientas

La respuesta repite las fases de la unidad anterior (aislar, erradicar, recuperar). Como apoyo se usan herramientas forenses, plataformas de gestión de respuesta que reparten tareas y llevan el control de lo hecho (por ejemplo, ServiceNow o PagerDuty) y las copias de seguridad. Son solo ejemplos: las herramientas cambian con el tiempo.

4 Comunicar durante el incidente

COMUNICACIÓN INTERNA

Informar al personal clave (TI, seguridad, dirección) y dar instrucciones claras a los empleados: desconectar su equipo, cambiar contraseñas, etc.

COMUNICACIÓN EXTERNA

Avisar cuando proceda a autoridades (policía, regulador de protección de datos), clientes afectados o proveedores, siguiendo los procedimientos legales.

! CORREGIDO

El original cita la «Ley General de Protección de Datos (GDPR)». Las siglas GDPR corresponden al Reglamento General de Protección de Datos (RGPD en español), que es un reglamento europeo y no una ley. (Aviso añadido a este manual.)

5 Evaluación posterior

Con el incidente resuelto, conviene responder a tres preguntas: qué puntos débiles lo permitieron, qué funcionó bien en la respuesta y qué se puede mejorar, y cómo reforzar la seguridad para evitar que se repita.

UNIDAD XXIII

Copias de seguridad y recuperación de datos

Si un ransomware cifra los archivos, un disco falla o un incendio destruye el local, las **copias de seguridad** (respaldos) permiten seguir trabajando sin pérdidas graves. La **recuperación de datos** es el proceso inverso: restaurar la información desde la copia a su estado original después de que el incidente haya alterado o destruido los datos.

1 Tipos de copia

Tipo	Qué copia	Ventaja	Inconveniente
Completa	Todos los datos seleccionados en un momento dado.	Es la más segura y la restauración es la más sencilla.	Consume más espacio y tiempo.

Tipo	Qué copia	Ventaja	Inconveniente
Incremental	Solo lo que ha cambiado desde la última copia, sea completa o incremental.	Es rápida y ocupa poco.	Restaurar exige la completa más todas las incrementales sucesivas, por lo que es más lento.
Diferencial	Todo lo modificado desde la última copia completa.	Es más rápida que la completa y restaurar es más ágil que con incrementales.	Ocupa más que la incremental, porque los cambios se acumulan hasta la siguiente completa.

Además, según *dónde* se guarden:

EN LA NUBE

Los datos se almacenan en servidores remotos, accesibles desde cualquier lugar, con escalabilidad y redundancia geográfica.

LOCAL

Discos duros o cintas dentro de las instalaciones. La restauración es más rápida, pero una catástrofe local (incendio, inundación) puede destruir también la copia.

2 Estrategia: la regla 3-2-1

La estrategia debe adaptarse al tipo de datos y a sus riesgos. Una pauta muy extendida es la **regla 3-2-1**:

- **3 copias** de los datos: el original y dos copias de respaldo.
- **2 tipos de medio** distintos, por ejemplo un disco duro y la nube.
- **1 copia fuera del sitio**, para protegerse de desastres locales.

Conviene además **automatizar** las copias con herramientas que las programen (diarias, semanales...) y avisen si algo falla, para que no dependan de que alguien se acuerde.

3 Procedimiento de recuperación

- **Plan de recuperación ante desastres (DRP):** procedimientos documentados para recuperar la infraestructura de TI, incluidos los datos. Debe probarse con regularidad y mantenerse actualizado.
- **Restauración completa:** se recupera todo desde una copia completa; es más lenta, pero garantiza la integridad.
- **Restauración selectiva:** se recuperan solo ciertos archivos o bases de datos; es más rápida cuando no hace falta todo.
- **Verificación de integridad:** tras restaurar, hay que comprobar que los datos no están corruptos y son utilizables.

4 Proteger también las copias

Las copias son un objetivo atractivo para los atacantes, así que su seguridad es tan importante como la de los datos originales.

- **Cifrado** en tránsito (cuando se envían) y en reposo (cuando se almacenan).
- **Control de acceso** restringido a personas autorizadas, con registro de las acciones realizadas sobre las copias.
- **Nube segura:** elegir proveedores con cifrado, autenticación multifactor (MFA) y auditorías periódicas.

5 Probar las copias

Una copia que nunca se ha restaurado es una apuesta, no una garantía. El temario recomienda hacer **pruebas de restauración al menos una vez al año** (o más a menudo, si es posible) y realizar **simulacros de recuperación ante desastres** para comprobar que la organización responde con rapidez.

UNIDAD XXIV

Simulacros y pruebas de estrés

No se aprende a gestionar una crisis durante la crisis. Dos tipos de ejercicio ayudan a prepararse:

SIMULACRO DE INCIDENTE

Imita un ataque o una crisis para entrenar la respuesta de las personas y los equipos.

PRUEBA DE ESTRÉS

Somete la infraestructura (red, servidores, aplicaciones) a condiciones extremas, como un aumento brusco de tráfico, para ver si aguanta.

1 Simulacros de incidentes

Según su forma

- **Tabletop (teórico):** los equipos debaten cómo responderían a un escenario (ransomware, phishing, filtración) sin tocar los sistemas. Sirve para evaluar la coordinación y la toma de decisiones.
- **De respuesta activa:** se recrea el incidente en tiempo real y los equipos actúan como si fuera cierto: desconectan sistemas, monitorizan, se comunican con los afectados y restauran.

Según su alcance

Simulacro	Qué entrena
De respuesta de TI	Aislar sistemas, aplicar parches y restaurar datos.
De respuesta de negocio	Cómo mantienen la continuidad los equipos no técnicos (finanzas, recursos humanos, operaciones) ante una interrupción del servicio.
Completo (full-scale)	La coordinación de todos los departamentos y la gestión de la crisis a nivel de toda la organización.

Sirven para detectar puntos débiles, comprobar si el plan de respuesta (IRP) funciona, mejorar la comunicación y practicar sin el riesgo de un ataque real.

2 Pruebas de estrés de sistemas

Prueba	Qué hace
De carga	Simula más tráfico o solicitudes de lo normal para ver cómo se comporta la infraestructura ante una sobrecarga, por ejemplo un ataque DDoS.
De capacidad	Mide el rendimiento con distintas cargas para conocer el límite: usuarios simultáneos, transacciones o datos que se pueden procesar sin degradarse.
De desbordamiento (*stress testing*)	Empuja el sistema más allá de su capacidad máxima para ver cómo se comporta y cómo se recupera al llegar al límite.

Con ellas se descubren **cuellos de botella** (componentes que fallan o se ralentizan con carga alta), se mejora la resiliencia y se comprueba que los protocolos de recuperación funcionan incluso con mucha demanda.

> **! IMPORTANTE**
> Las pruebas de estrés se hacen solo sobre sistemas propios o con autorización expresa, y coordinadas con quien los gestiona. Lanzar una sobrecarga contra sistemas ajenos es un ataque. (Aviso añadido a este manual.)

3 Cómo planificar y ejecutar

1. **Define objetivos claros**, por ejemplo evaluar la respuesta a un ataque concreto o medir el tiempo de recuperación.
2. **Implica a todos los equipos relevantes:** TI, comunicaciones, recursos humanos y legal.
3. **Repítelos con regularidad**, para que los procedimientos se actualicen y los equipos sigan preparados.
4. **Analiza el resultado:** qué se hizo bien, qué falló y qué hay que mejorar.

UNIDAD XXV

Reporte de incidentes y comunicación con las autoridades

Notificar un incidente a tiempo ayuda a reducir sus consecuencias, aporta transparencia y permite cumplir la ley. El reporte incluye tanto el aviso interno como la comunicación con entidades externas: autoridades de protección de datos, reguladores sectoriales y, en algunos casos, las fuerzas de seguridad.

1 Cuándo hay que reportar

Siempre que ocurra algo que pueda comprometer la confidencialidad, integridad o disponibilidad de sistemas, redes o datos. Por ejemplo:

- Ataques como ransomware, malware o DDoS.
- Filtración o pérdida de datos sensibles.
- Acceso no autorizado a sistemas o información.
- Vulnerabilidades graves descubiertas en los sistemas.
- Incidentes que paralicen servicios críticos.

2 Proceso interno

Antes de avisar fuera se sigue el protocolo interno: detección, notificación inmediata al equipo de respuesta (CSIRT o equipo de seguridad), evaluación del alcance y el impacto, contención y remediación, e informe interno formal con las acciones realizadas y las lecciones aprendidas.

3 A quién se informa

Depende de la naturaleza del incidente, del sector y de la jurisdicción.

PROTECCIÓN DE DATOS

Si hay filtración o acceso no autorizado a datos personales, el temario indica que la notificación a la Agencia Española de Protección de Datos (AEPD) es obligatoria según el RGPD.

FUERZAS DE SEGURIDAD

Ante un ataque grave o una actividad delictiva, se puede acudir a la Guardia Civil o a la Policía Nacional, que cuentan con unidades especializadas en delitos informáticos.

REGULADORES DEL SECTOR

En banca, salud o telecomunicaciones, ciertos incidentes deben comunicarse a la autoridad sectorial (el temario cita el Banco de España, la CNMV y la Agencia Española de Medicamentos y Productos Sanitarios).

4 Cómo se notifica a una autoridad

1. **Identifica la autoridad competente:** la AEPD para filtraciones de datos personales, o un CERT (equipo de respuesta a emergencias informáticas) para ciberataques.
2. **Reúne la información:** descripción detallada, impacto (datos y sistemas afectados), medidas de contención adoptadas y cronología de los hechos.
3. **Notifica formalmente** por el canal que establezca la autoridad (correo, formulario web, teléfono...) y dentro del plazo, si lo hay.

4 **Colabora en la investigación** facilitando los datos adicionales que se soliciten.

5 Obligaciones legales según el temario

- **RGPD:** ante una violación de datos personales, la organización debe notificarla a la autoridad de protección de datos competente **dentro de las 72 horas siguientes a detectarla**, salvo que sea improbable que suponga un riesgo para los derechos y libertades de las personas. El temario lo atribuye al artículo 33.
- **LSSI-CE (Ley 34/2002):** el temario indica que las empresas prestadoras de servicios electrónicos deben comunicar a las autoridades pertinentes, como el CERT, los incidentes que afecten a la seguridad de sus servicios.

! CORREGIDO

El original menciona la LSSI-CE dos veces, una con su número (Ley 34/2002) y otra sin él, con redacciones casi idénticas. Se han fusionado en un único punto. (Aviso añadido a este manual.)

! DATO ACTUALIZADO

Los plazos y los sujetos obligados a notificar dependen de la normativa vigente y de cada sector, y pueden haber cambiado desde que se redactó el temario. Comprueba la normativa vigente en el BOE y en la AEPD antes de actuar. (Aviso añadido a este manual.)

6 Comunicación con los usuarios afectados

Además de avisar a las autoridades, la organización puede estar obligada a informar a las personas afectadas, sobre todo si se han comprometido sus datos personales. El RGPD pide hacerlo de forma clara y comprensible: qué ha pasado, cuáles pueden ser las consecuencias y qué medidas se han tomado para reducir el riesgo.

7 Buenas prácticas

Actúa con rapidez y transparencia, documenta todo el proceso y comparte la información sensible solo con quien deba conocerla (autoridades, afectados).

! RECUERDA

Ante un incidente: detecta, contén, erradica, recupera y aprende, documentándolo todo, y avisa a quien corresponda a tiempo (en una violación de datos personales, en 72 horas según el temario). Y no confíes en una copia de seguridad que nunca hayas probado a restaurar.

MÓDULO VI

Seguridad en la nube y el comercio electrónico

Cada vez más datos y negocios viven en servicios de terceros y se mueven por internet. Este módulo explica los riesgos de la nube y cómo reducirlos, cómo el cifrado protege la información, cómo se asegura una aplicación web, cómo se protegen los pagos online y qué normas y principios éticos debes respetar.

UNIDAD XXVI

Riesgos asociados al uso de servicios en la nube

Los servicios en la nube permiten acceder de forma remota y flexible a aplicaciones, almacenamiento y capacidad de proceso sin montar una infraestructura propia. A cambio, parte del control pasa al proveedor, y eso introduce riesgos que hay que gestionar.

1 Modelos de servicio

SAAS · SOFTWARE COMO SERVICIO

El proveedor ofrece y gestiona la aplicación completa. Ejemplos: Google Workspace o Microsoft 365.

PAAS · PLATAFORMA COMO SERVICIO

El proveedor da las herramientas para que los desarrolladores creen y ejecuten sus aplicaciones. Ejemplos: Google App Engine o Microsoft Azure.

IAAS · INFRAESTRUCTURA COMO SERVICIO

El proveedor alquila recursos básicos, como almacenamiento y redes. Ejemplos: Amazon Web Services (AWS) o Microsoft Azure.

Cuanto más bajas de SaaS a IaaS, más control y más responsabilidad de seguridad asumes tú (idea añadida a este manual). Los nombres de productos son solo ejemplos y cambian con el tiempo.

! CORREGIDO

El temario cita Microsoft Azure como ejemplo de PaaS y de IaaS. No es un error: la misma plataforma ofrece ambos tipos de servicio.

2 Riesgos principales

Riesgo	En qué consiste
Privacidad y protección de datos	Los datos están fuera de tu infraestructura: pueden quedar accesibles a terceros por controles de acceso deficientes o estar sujetos a leyes de otros países. Hay que comprobar que el proveedor cumple la normativa de protección de datos (por ejemplo, el GDPR en Europa).
Pérdida de datos	Un fallo del proveedor o un incidente puede destruir información. Muchas empresas no configuran sus propias copias de seguridad y dependen solo del proveedor.
Vulnerabilidades del entorno compartido	En un entorno multiarrendatario (*multi-tenant*) varios clientes comparten recursos; un fallo en esa base común podría afectar a todos. Además, tienes poca visibilidad de los controles que aplica el proveedor.
Interrupción del servicio	Fallos técnicos o mantenimientos pueden dejarte sin acceso. Si el proveedor tiene problemas graves o desaparece, te quedas sin aplicaciones ni datos (dependencia de terceros).
Ciberataques	Al estar conectada a internet, la nube sufre ataques de denegación de servicio (DDoS), inyección de código, robo de credenciales, malware y ransomware.
Control y gobernanza	Es difícil controlar cómo se tratan los datos cuando se reparten en varias ubicaciones geográficas, con implicaciones legales sobre la soberanía de los datos.

3 Cómo mitigarlos

Los riesgos no se eliminan del todo, pero se reducen mucho con estas medidas:

- **Cifrar** los datos en tránsito y en reposo (se explica en la siguiente unidad).
- **Gestionar identidades y accesos (IAM)**: control de acceso robusto y autenticación multifactor, para que solo entre quien debe.
- **Elegir bien al proveedor**: que cumpla estándares reconocidos, como ISO 27001 o SOC 2, y tenga un historial de seguridad contrastado.
- **Hacer copias de seguridad propias** y probar periódicamente que se pueden restaurar.
- **Auditar** la seguridad y las vulnerabilidades con regularidad.
- **Revisar el SLA** (acuerdo de nivel de servicio): debe fijar compromisos de disponibilidad, tiempo de respuesta ante incidentes y medidas de seguridad.

UNIDAD XXVII

Cifrado de datos en la nube

El cifrado convierte los datos en un formato ilegible sin la clave adecuada. Si alguien los intercepta o los roba, no puede leerlos ni usarlos. En la nube se aplica en dos estados de los datos, y existe un tercer

enfoque más estricto: el cifrado de extremo a extremo.

1 Datos en reposo

Son los datos almacenados en discos, bases de datos u otros soportes mientras nadie los usa ni los transmite.

- Si un atacante accede al almacenamiento, no puede leer los datos sin la clave.
- Ayuda a cumplir normativas como GDPR, HIPAA o PCI-DSS.
- Limita lo que ven empleados o proveedores con acceso al sistema: solo quien tenga la clave puede leer el contenido.

Técnicas habituales

- **AES (Advanced Encryption Standard)**: el estándar más usado, con claves de 128, 192 o 256 bits.
- **Cifrado a nivel de archivo**: se cifra cada archivo por separado.
- **Cifrado de disco completo**: se cifra todo el almacenamiento, incluido el sistema operativo y las aplicaciones.

Algunos proveedores, como AWS (con su servicio de claves KMS) o Google Cloud (que cifra en reposo por defecto), ya lo incorporan.

2 Datos en tránsito

Son los datos que viajan entre sistemas, por ejemplo entre un usuario y un servidor en la nube. Es esencial en redes públicas o poco seguras. Protege frente a la interceptación, garantiza que los datos no se alteran por el camino (integridad) y es exigido por muchas normativas.

Protocolo	Para qué sirve
TLS	Es el protocolo más común; es la base de HTTPS, que protege la comunicación entre navegador y servidor web (compras, banca online...).
SSL	Predecesor de TLS. Está obsoleto, aunque aún aparece en algunos sistemas; hoy se prefiere TLS.
VPN	Crea un canal cifrado entre el dispositivo y los servidores; muy útil para el teletrabajo.
IPsec	Cifra el tráfico a nivel de red entre redes, servidores y dispositivos.
SSH	Cifra las sesiones de acceso remoto a servidores y evita que se intercepten contraseñas y órdenes.

3 Cifrado de extremo a extremo (E2EE)

Los datos se cifran en el dispositivo del emisor y solo se descifran en el del receptor. Los servidores intermedios no tienen las claves, de modo que ni siquiera el proveedor puede leer el contenido, y una brecha en su infraestructura no expone los datos en claro. Lo usan aplicaciones de mensajería como Signal o WhatsApp.

CORREGIDO

El temario describe el E2EE como cifrado «desde el dispositivo del usuario hasta el servidor de la nube». Eso es cifrado en tránsito hasta el servidor. En el cifrado de extremo a extremo los dos extremos son las personas (o dispositivos) que se comunican, y el servidor solo ve datos cifrados.

4 Buenas prácticas

- **Gestionar bien las claves** con un sistema específico (por ejemplo, AWS KMS o Azure Key Vault), accesible solo para personal autorizado. Si pierdes o filtras la clave, el cifrado no sirve.
- **Cifrar durante todo el ciclo de vida** de los datos: creación, almacenamiento y transmisión.
- **Controlar el acceso** a las claves y a los datos cifrados, tanto de usuarios como de aplicaciones.

UNIDAD XXVIII

Seguridad en aplicaciones web

Las aplicaciones web son accesibles desde cualquier lugar, y por eso son objetivo prioritario de los ciberdelincuentes. Una aplicación vulnerable puede exponer datos de los usuarios, alterar información y dar acceso a sistemas internos.

1 Amenazas habituales

INYECCIÓN SQL

Se aprovechan entradas de usuario sin validar para manipular las consultas a la base de datos y acceder a información confidencial.

CROSS-SITE SCRIPTING (XSS)

Se consigue que las páginas muestren código malicioso a otros usuarios, con el fin de robar credenciales o actuar en su nombre.

CSRF

Se engaña a un usuario ya autenticado para que ejecute acciones que no quería, como una compra o un cambio de configuración.

EXPOSICIÓN DE DATOS SENSIBLES

Sin cifrado adecuado, contraseñas o datos personales pueden ser interceptados y leídos.

AUTENTICACIÓN INSEGURA

Contraseñas débiles o ausencia de MFA permiten el acceso no autorizado a cuentas.

2 Buenas prácticas de desarrollo

La seguridad debe tenerse en cuenta en todas las fases del desarrollo, no añadirse al final.

- **Validar y sanear todas las entradas** del usuario, aceptando solo los tipos de datos esperados.

- **Usar consultas preparadas u ORM**, que separan la consulta de los datos del usuario y evitan la inyección SQL.
- **Cifrar datos sensibles** en tránsito (TLS/HTTPS) y en reposo (AES), y guardar las contraseñas como hash con algoritmos pensados para ello, como bcrypt.
- **Autenticación y autorización seguras**, con estándares como OAuth, JWT u OpenID Connect y con el principio de privilegios mínimos.
- **MFA**: pedir un segundo factor (aplicación de autenticación o código enviado) reduce mucho el riesgo de acceso indebido.
- **Evitar componentes vulnerables**: mantener actualizados bibliotecas y frameworks y revisar las dependencias con herramientas como OWASP Dependency-Check.
- **Gestionar bien las sesiones**: identificadores aleatorios y seguros, caducidad y cierre de las sesiones inactivas para evitar el secuestro de sesión.

3 Arquitectura segura

- **Defensa en profundidad**: varias capas (cortafuegos, IDS/IPS, protección a nivel de aplicación) para que, si una falla, otra siga protegiendo.
- **Seguridad de las API**: protegerlas frente a inyección, falsificación de peticiones y fugas de información, con pasarelas de API seguras y control de acceso que limite las solicitudes.
- **Microservicios**: cada uno aislado y con su propio control de acceso, con comunicaciones cifradas y autenticadas.
- **Configuración del servidor web**: desactivar mensajes de error detallados que revelen datos del sistema y proteger los directorios de la aplicación.

4 Pruebas y auditorías

- **Pruebas de penetración (*pentesting*)**: profesionales autorizados simulan ataques para descubrir puntos débiles antes que los delincuentes.
- **Escaneo de vulnerabilidades**: herramientas automáticas (por ejemplo OWASP ZAP o Burp Suite) detectan fallos comunes.
- **Análisis de código fuente**: el análisis estático busca vulnerabilidades como inyecciones, datos expuestos o bibliotecas inseguras.

> **! RECUERDA**
>
> Las herramientas cambian con el tiempo; lo importante es hacer estas pruebas de forma periódica y solo sobre sistemas para los que tengas autorización.

UNIDAD XXIX

Seguridad en las transacciones electrónicas

Una transacción electrónica es cualquier operación financiera hecha por medios digitales: pagos online, transferencias o compras en una tienda web. Implica datos personales, bancarios y de pago, por lo que

el auge del comercio electrónico ha traído también más riesgo de fraude y robo de datos.

1 Amenazas

- **Phishing y *spoofing***: correos o webs falsos que imitan a entidades legítimas para que entregues credenciales o datos de pago.
- **Man-in-the-Middle (MITM)**: el atacante se interpone en la comunicación entre usuario y servidor para robar datos como números de tarjeta.
- **Skimming**: copia de los datos de tarjetas, sobre todo en terminales físicos manipulados.
- **Ransomware**: secuestra los datos, incluidos los de pago, y exige un rescate.

2 Medidas de protección

CIFRADO SSL/TLS Y HTTPS

Protege la confidencialidad e integridad de los datos entre el navegador y la tienda.

2FA / MFA

Exige dos o más factores para verificar la identidad, por ejemplo contraseña y código en el móvil.

TOKENIZACIÓN

Sustituye el número de tarjeta por un token único, de modo que se paga sin exponer los datos reales.

FIRMA DIGITAL

Verifica que la transacción es auténtica, que su origen es legítimo y que no se ha modificado en el camino.

3 Estándares y normas

Norma	Qué exige
PCI DSS	Estándar de la industria de tarjetas: quien procesa pagos con tarjeta debe cifrar los datos, autenticar de forma segura y someterse a auditorías periódicas.
GDPR (RGPD)	Regula el tratamiento de datos personales, también en los pagos; exige consentimiento explícito antes de tratarlos.
PSD2	Directiva europea de servicios de pago que obliga a las entidades financieras a aplicar la autenticación reforzada de cliente (SCA).

4 Buenas prácticas para comerciantes online

- **Verificar la identidad del comprador**, por ejemplo con doble factor.
- **Monitorizar transacciones** en tiempo real para detectar patrones raros (ubicación, importes, frecuencia).
- **Usar plataformas de pago de confianza** (como PayPal o Stripe, a modo de ejemplo) en lugar de gestionar tú mismo los datos de tarjeta.

- **Educar al cliente** para que reconozca estafas, correos de phishing y webs fraudulentas.

UNIDAD XXX

Consideraciones legales y éticas

La nube y el comercio electrónico están sujetos a normas sobre datos personales, transacciones y servicios online. Estas normas varían según el país y el sector, así que conviene conocer las que te afectan y añadir unos principios éticos claros.

1 Protección de datos personales

- **GDPR (RGPD) de la UE**: una de las normativas más estrictas del mundo. Exige consentimiento explícito para recoger y tratar datos, reconoce los derechos de acceso, rectificación y supresión, y obliga a notificar las brechas de seguridad en un plazo determinado.
- **CCPA de California**: derechos parecidos para los residentes de ese estado de EE. UU.: saber qué datos se recogen, pedir su eliminación y negarse a que se vendan.
- **Datos en la nube**: el proveedor también debe cumplir la normativa; se formaliza con un acuerdo de tratamiento de datos (DPA) que detalle cómo se gestionan, almacenan y protegen.

DATO ACTUALIZADO

Si en otros materiales ves citada la «LOPD», está desfasada. Hoy rigen el RGPD/GDPR y la ley orgánica española que lo complementa. Comprueba siempre la normativa vigente en el BOE y en la AEPD.

2 Comercio electrónico y firma electrónica

- **LSSI-CE (Ley de servicios de la sociedad de la información y de comercio electrónico)**: en España regula la actividad comercial online. Obliga a dar información clara sobre productos, precios, condiciones de venta y devoluciones, y regula el marketing digital, como los correos comerciales.
- **Firma electrónica**: marco legal para firmar transacciones por medios electrónicos. Los sistemas de firma deben ser seguros y cumplir la normativa nacional e internacional. Comprueba la normativa vigente, pues ha cambiado con el tiempo.
- **Pagos y fraude**: la PSD2 regula la seguridad de los pagos electrónicos, con autenticación reforzada (SCA), y obliga a los comerciantes a aplicar medidas adicionales.

3 Principios éticos

TRANSPARENCIA

Explicar con claridad cómo se recogen, guardan y tratan los datos y qué condiciones se aceptan.

EQUIDAD Y NO DISCRIMINACIÓN

Prácticas justas y acceso igualitario a los servicios, sin prejuicios por raza, género, orientación sexual u otra característica personal.

CONFIDENCIALIDAD Y PRIVACIDAD

Guardar los datos de forma segura, no usarlos para fines no autorizados y dar al usuario control sobre ellos.

RESPONSABILIDAD SOCIAL

Ir más allá de la ley y contribuir al bienestar social y medioambiental, con un uso responsable de la tecnología.

4 Derechos del consumidor

- **Información** completa y veraz sobre precio, características, plazos de entrega y devoluciones.
- **Consentimiento informado** para recoger y usar sus datos, sin engaños ni presiones para aceptar términos que no entiende.
- **Seguridad** al comprar: la tienda debe aplicar cifrado TLS, autenticación multifactor y otros mecanismos.

! RECUERDA

En la nube compartes la responsabilidad con el proveedor: cifra, controla accesos y haz tus propias copias. En el comercio online combina HTTPS, doble factor y tokenización, y cumple la normativa de protección de datos y de pagos vigente.

MÓDULO VII

Seguridad informática y gestión de la información

Este módulo aclara qué se entiende por ciberseguridad y por seguridad de la información, explica los tres principios sobre los que se apoya toda la protección de datos y repasa la normativa, la clasificación de la información sensible y la forma de planificar una auditoría.

AVISO

El temario usa «seguridad informativa» y «LOPD». En este manual se escribe **seguridad informática** o **seguridad de la información**, y la normativa se explica con la referencia vigente (ver la nota «Dato actualizado» de la Unidad XX sobre protección de datos). Las herramientas que se citan son solo ejemplos y cambian con el tiempo.

UNIDAD XXXI

Ciberseguridad y seguridad informática: definiciones y diferencias

1 Qué es la ciberseguridad

La **ciberseguridad** es el conjunto de prácticas, tecnologías y procesos que protegen sistemas, redes y datos frente a ataques, daños y accesos no autorizados en el entorno digital. Su meta es garantizar la confidencialidad, la integridad y la disponibilidad de los recursos tecnológicos de una organización. Abarca cuatro frentes:

- **Protección de redes:** evitar intrusiones y accesos maliciosos.
- **Defensa contra ciberataques:** phishing, ransomware, malware y denegación de servicio.
- **Control de accesos:** que solo entren los usuarios autorizados.
- **Seguridad de aplicaciones y dispositivos:** que el software y los equipos resistan los ataques.

2 Qué es la seguridad informática (o de la información)

Es un enfoque más amplio: protege la **información en cualquier forma**, digital o física, y dondequiera que esté almacenada o por donde circule. Incluye, por ejemplo, guardar bajo llave los documentos en papel, controlar quién accede a la información confidencial y formar al personal en el manejo de datos.

CORREGIDO

El original escribe «seguridad informativa» en toda la lección; el término correcto es «seguridad informática» (o «seguridad de la información»). (Aviso añadido a este manual.)

3 Diferencias clave

Aspecto	Ciberseguridad	Seguridad de la información
Enfoque	Protección frente a ciberataques y amenazas digitales.	Protección de la información en todas sus formas, física y digital.
Ámbito	Sistemas, redes, aplicaciones y dispositivos; sobre todo el ciberespacio.	Toda la información de la organización, esté donde esté.
Amenazas	Hackers, malware, virus y otros riesgos tecnológicos.	Accesos no autorizados, manipulación o pérdida de datos, internos y externos.
Medidas típicas	Cortafuegos, cifrado, autenticación multifactor.	Políticas de gestión, control de acceso, clasificación de la información.

La ciberseguridad es, en la práctica, **una parte de la seguridad de la información**. Por ejemplo, la ciberseguridad defiende la red de la empresa contra un ataque de phishing; la seguridad de la información añade que los documentos confidenciales solo los vean empleados autorizados y que las reuniones donde se tratan datos sensibles se hagan en un entorno seguro. Un fallo en un área puede comprometer la otra, así que conviene combinar herramientas (cortafuegos, antivirus, cifrado) con políticas internas (accesos, formación, supervisión de datos).

UNIDAD XXXII

Principios de la protección de datos: la tríada CIA

La **tríada CIA** (por sus siglas en inglés: *Confidentiality, Integrity, Availability*) es el modelo base de la seguridad de la información. Cada principio se apoya en mecanismos concretos.

1 Confidencialidad

Solo pueden acceder a la información las personas o entidades autorizadas. Es clave para datos personales, propiedad intelectual y datos empresariales reservados.

- **Cifrado** de los datos en tránsito y en reposo.
- **Control de acceso:** contraseñas robustas, autenticación multifactor (MFA) y permisos por roles (RBAC).
- **Políticas** de manejo de datos sensibles.

> **! EJEMPLO**
>
> Un hospital permite consultar los historiales clínicos solo al personal médico autorizado, con doble factor de autenticación y registros cifrados.

2 Integridad

La información no se altera, destruye ni manipula sin autorización, y se mantiene completa, exacta y coherente durante todo su ciclo de vida.

- **Sumas de comprobación (hash):** detectan si un dato ha cambiado.
- **Control de versiones:** permite seguir los cambios y recuperar una versión anterior.
- **Registros de auditoría:** dejan rastro de quién modificó qué.

3 Disponibilidad

Los usuarios autorizados pueden acceder a los datos y sistemas cuando los necesitan, incluso con mucha demanda o en una crisis.

- **Copias de seguridad** regulares y plan de recuperación.
- **Redundancia** de servidores, redes y bases de datos.
- **Planes de continuidad de negocio (BCP)** para seguir funcionando durante y después de un incidente.

4 Cómo se relacionan

Los tres principios dependen unos de otros: si falla uno, los demás se resienten.

CONFIDENCIALIDAD ROTA

Un phishing que roba credenciales puede acabar en datos robados o manipulados, es decir, afecta también a la integridad.

DISPONIBILIDAD ROTA

Un ataque de denegación de servicio (DoS) corta el acceso y puede dejar la información expuesta o incompleta.

UNIDAD XXXIII

Normativa de protección de datos: RGPD y legislación española

1 Marco normativo

El **RGPD** (Reglamento General de Protección de Datos, GDPR en inglés) es la norma de la Unión Europea que regula el tratamiento de los datos personales con el fin de reforzar la privacidad de las personas. En España lo complementa una ley orgánica nacional, que el temario llama «LOPD».

! DATO ACTUALIZADO

El nombre «LOPD» corresponde a una norma antigua; hoy rigen el RGPD y la ley orgánica española que lo complementa. Comprueba siempre la normativa vigente en el BOE y en la web de la AEPD (Agencia Española de Protección de Datos). (Aviso añadido a este manual.)

2 Qué exige el RGPD

- **Consentimiento** explícito e informado antes de tratar datos personales.
- **Derecho de acceso:** la persona puede saber qué datos se tienen de ella y para qué se usan.
- **Rectificación:** corregir datos incorrectos o incompletos.
- **Supresión («derecho al olvido»):** pedir que se eliminen, en ciertas condiciones.

- **Portabilidad:** solicitar que los datos pasen a otro proveedor.
- **Minimización:** recoger solo los datos necesarios para la finalidad declarada.
- **Protección desde el diseño y por defecto:** integrar la seguridad desde el principio en sistemas y procesos.

El temario añade, como obligaciones asociadas a la normativa española, el **registro de actividades de tratamiento**, el nombramiento de un **Delegado de Protección de Datos (DPO)** en las organizaciones que lo requieran y la **evaluación de impacto (DPIA)** para ciertos tratamientos de riesgo.

3 Pasos para cumplir

1. **Auditar los datos personales:** qué se recoge, cómo se guarda, quién accede y durante cuánto tiempo.
2. **Obtener el consentimiento** con formularios claros; debe ser específico, informado y revocable.
3. **Aplicar medidas de seguridad:** cifrado, control de acceso, autenticación fuerte y copias de seguridad.
4. **Publicar una política de privacidad** clara y accesible.
5. **Formar al personal** en el manejo seguro de datos personales.
6. **Designar un DPO** si corresponde, como punto de contacto para los afectados y las autoridades.
7. **Habilitar el ejercicio de derechos:** acceso, rectificación, supresión y portabilidad.

4 Brechas de seguridad y sanciones

Si ocurre una brecha que afecta a datos personales, la organización debe **notificarla a la autoridad de protección de datos en un máximo de 72 horas** desde que la conoce e **informar a las personas afectadas** cuando suponga un alto riesgo para sus derechos y libertades.

Según el temario, las infracciones graves pueden sancionarse con multas de hasta 20 millones de euros o el 4 % de la facturación anual global (la mayor), además de reclamaciones de los afectados y daño a la reputación. Plazos e importes proceden del temario: verifícalos en la AEPD o el BOE.

UNIDAD XXXIV

Clasificación y protección de la información sensible

1 Qué es información sensible

Es cualquier dato cuyo acceso o divulgación no autorizados puedan causar daño a una persona o a una organización. Por eso merece una protección más estricta. Sus tipos principales:

- Datos personales y de salud (identidad, contacto, historias clínicas).
- Información financiera (cuentas, tarjetas, historial crediticio).

- Propiedad intelectual (patentes, diseños, código fuente).
- Datos confidenciales de empresa (estrategias, auditorías, contratos).

2 Niveles de clasificación

Clasificar es agrupar la información según su sensibilidad y asignar a cada grupo los controles adecuados. La clasificación debe ser clara, coherente y ajustarse a las normas de la organización y a la ley.

Nivel	Qué es	Ejemplos
Público	Se puede compartir sin restricciones.	Material de marketing, contenido web público.
Interno	Acceso restringido a la plantilla; su divulgación no causa daños significativos.	Comunicaciones y procedimientos internos.
Confidencial	Su divulgación podría dañar a la organización o a personas.	Contratos, informes financieros.
Secreto	Extremadamente sensible; su filtración tendría consecuencias graves.	Información de clientes clave, investigación y desarrollo.

3 Cómo protegerla

PROTECCIÓN FÍSICA

Control de acceso a las instalaciones y archivo de documentos en armarios cerrados o cajas fuertes.

PROTECCIÓN LÓGICA

Cifrado en reposo y en tránsito, acceso según el **mínimo privilegio** (solo quien lo necesita para su trabajo) y autenticación multifactor.

COMUNICACIONES

Protocolos seguros (HTTPS, TLS) y VPN para accesos remotos.

CONTROL Y RETENCIÓN

Registros de actividad para detectar accesos sospechosos y políticas que fijen cuánto se conservan los datos y cómo se eliminan de forma segura.

4 Normas y desafíos

- **RGPD:** exige medidas como la anonimización, el cifrado y la protección contra accesos no autorizados.
- **ISO 27001:** norma internacional para implantar y mejorar un sistema de gestión de seguridad de la información (SGSI).
- **Legislación española:** añade disposiciones nacionales (véase la unidad anterior).

Los principales desafíos son las **amenazas internas** (accidentales o malintencionadas), los **ataques externos** (phishing, ransomware) y la **complejidad** de gestionar grandes volúmenes de datos sensibles.

UNIDAD XXXV

Planificación de auditorías de seguridad de la información

1 Qué es una auditoría y qué tipos hay

Una **auditoría de seguridad** es una revisión formal de los sistemas, políticas y controles de una organización para comprobar que la información se maneja y protege bien. Sirve para evaluar la eficacia de las políticas, verificar el cumplimiento de leyes y estándares, detectar fallos y proponer mejoras.

Según quién la hace y qué evalúa, puede ser **interna** (personal propio) o **externa** (entidad ajena, más objetiva), y de **cumplimiento** (RGPD, ISO 27001), de **riesgos** o de **infraestructura** (servidores, redes, dispositivos).

2 Cómo se planifica

1. **Definir el alcance:** qué sistemas de TI, políticas y procedimientos, requisitos normativos y aspectos físicos se auditan.
2. **Fijar objetivos** concretos y alineados con la organización (por ejemplo, evaluar el control de accesos o la integridad de los sistemas).
3. **Identificar recursos:** equipo auditor (interno o externo), herramientas y un calendario que no frene la actividad diaria.
4. **Elegir metodología:** ISO 27001 para auditar un SGSI, NIST (directrices de evaluación de riesgos y controles) o CIS (controles específicos para redes y sistemas), según los objetivos.

3 Cómo se ejecuta

- **Revisión de políticas y procedimientos:** que estén documentados, actualizados y alineados con la normativa.
- **Análisis de vulnerabilidades y pruebas de penetración:** evaluaciones técnicas autorizadas y acordadas de antemano, junto con la revisión de configuraciones de red y sistemas.
- **Entrevistas y encuestas** al personal clave para comprobar cómo se aplican las políticas y el nivel de concienciación.
- **Revisión de controles físicos** de las instalaciones.

4 Informe y seguimiento

El informe final recoge los **hallazgos** (vulnerabilidades, deficiencias o incumplimientos), la **evaluación de riesgos** de cada uno (impacto y probabilidad) y las **recomendaciones** de mejora. Es la base para tomar decisiones.

La auditoría no es un hecho aislado: define **planes de acción** concretos, mantener una **monitorización continua** para que las vulnerabilidades no se aprovechen antes de corregirse y hacer **reevaluaciones periódicas** frente a nuevas amenazas y normativas.

Como ejemplos de herramientas de apoyo: escáneres de vulnerabilidades (Nessus, OpenVAS), analizadores de tráfico de red (Wireshark) y distribuciones con utilidades de auditoría (Kali Linux). Úsalas solo con autorización expresa sobre los sistemas auditados; las herramientas cambian con el tiempo.

> **! RECUERDA**
>
> La ciberseguridad es una parte de la seguridad de la información, que protege los datos en cualquier formato apoyándose en confidencialidad, integridad y disponibilidad. Clasifica la información, cumple la normativa vigente y audita de forma periódica.

MÓDULO VIII

Buenas prácticas y herramientas

Este módulo reúne las buenas prácticas del día a día y las herramientas que las hacen posibles: cómo configurar navegadores y aplicaciones, cómo vigilar lo que ocurre en un sistema, qué tipos de herramientas de seguridad existen, cómo crear y guardar contraseñas y qué hábitos protegen tu vida digital, personal y profesional.

! AVISO

Las herramientas y los productos que se citan son solo ejemplos para entender cada categoría. Cambian, desaparecen o se actualizan con frecuencia, así que comprueba siempre su estado actual antes de elegir una.

UNIDAD XXXVI

Configuración segura de navegadores y aplicaciones

El navegador y las aplicaciones son las puertas por las que interactuamos con internet y, por eso mismo, un objetivo habitual: los atacantes buscan fallos en ellos para robar datos, instalar malware o lanzar ataques de phishing. Una buena configuración reduce mucho ese riesgo y es una de las primeras barreras de defensa.

1 Navegadores web

ACTUALIZACIÓN AUTOMÁTICA

Las actualizaciones corrigen vulnerabilidades conocidas. Activa la actualización automática para no depender de acordarte.

NAVEGACIÓN PRIVADA

El modo incógnito evita que el navegador guarde historial, cookies, contraseñas y formularios en ese equipo. Mejora la privacidad local, pero no te hace anónimo en internet.

COOKIES Y RASTREO

Bloquea las cookies de terceros (las que más se usan para el rastreo) o configura el navegador para que te pregunte. Activa también la opción «no rastrear» en los ajustes de privacidad.

SITIOS PELIGROSOS

Mantén activa la protección integrada que avisa de sitios de phishing o con malware (por ejemplo, Google Safe Browsing).

HTTPS

Prioriza las conexiones HTTPS, que cifran la comunicación entre el navegador y el sitio y evitan que alguien la intercepte.

CONTRASEÑAS Y 2FA

Usa un gestor de contraseñas o el relleno automático seguro del navegador, y activa la verificación en dos pasos en las cuentas vinculadas.

2 Aplicaciones de escritorio y móviles

- **Actualízalas** y, siempre que se pueda, déjalas en modo automático.
- **Controla los permisos:** concede solo lo que la aplicación necesita para funcionar (ubicación, cámara, micrófono...). Si pide más de lo razonable, es una señal de alerta.
- **Protege el acceso:** contraseñas largas, complejas y únicas, y autenticación multifactor (MFA) donde esté disponible.
- **Evita las apps no seguras:** descarga solo desde tiendas oficiales (Google Play, App Store), evita tiendas de terceros y mantén un antivirus o antimalware en los dispositivos.
- **Ajusta la privacidad:** limita los datos que recopila la aplicación y, en redes sociales, quién puede ver tus publicaciones y contactos.
- **Prefiere apps que cifren** los datos sensibles (contraseñas, tarjetas...); si una no lo hace, busca una alternativa.

3 Extensiones y recomendaciones finales

Algunas extensiones refuerzan el navegador: los bloqueadores de anuncios y scripts maliciosos (como uBlock Origin), las que fuerzan HTTPS o las que bloquean rastreadores (como Privacy Badger). Instala pocas y de fuentes fiables, porque una extensión también tiene acceso a lo que haces en el navegador.

! DATO AÑADIDO

La extensión «HTTPS Everywhere» que cita el temario se dio por finalizada hace tiempo, porque los navegadores actuales ya incluyen un modo «solo HTTPS». Busca esa opción en los ajustes de seguridad de tu navegador. (Aviso añadido a este manual.)

- Evita el Wi-Fi público para operaciones sensibles; si no queda más remedio, usa una VPN.
- Audita de vez en cuando qué navegadores, extensiones y apps usas y qué permisos tienen.
- Mantente al día de las nuevas amenazas: la seguridad depende tanto de las herramientas como de los hábitos.

UNIDAD XXXVII

Monitorización y registro de actividades

Monitorizar es observar lo que ocurre en un sistema; registrar es dejar constancia de ello en **logs**. Juntos permiten detectar incidentes pronto, reconstruir qué pasó y demostrar que se cumplen las normas.

1 Para qué sirve

- **Detección temprana:** con la monitorización en tiempo real se ven intentos de intrusión, accesos no autorizados o comportamientos anómalos mientras suceden.
- **Trazabilidad:** los registros conservan el historial de acciones, imprescindible para investigar incidentes y hacer auditorías.
- **Cumplimiento normativo:** según el temario, normas como el GDPR o la ISO 27001 exigen políticas de monitorización y conservación de registros.

2 Qué se vigila y qué se registra

En tiempo real se vigilan sobre todo los **accesos y autenticaciones** (fallos repetidos, intentos no autorizados), los **cambios en archivos y configuraciones** sensibles y el **tráfico de red** (conexiones desde IP no autorizadas o picos anormales).

Tipo de registro	Qué contiene
Logs de autenticación	Intentos de acceso, con sus éxitos y fracasos.
Logs del sistema	Eventos del sistema operativo: inicio y parada de servicios, errores y advertencias.
Logs de aplicaciones	Funcionamiento de cada aplicación y actividad de los usuarios dentro de ella.

Para automatizar el trabajo existen tres familias de herramientas: los **SIEM** (*Security Information and Event Management*), que centralizan y analizan los registros de muchos sistemas para detectar patrones de ataque (ejemplos: Splunk, Graylog, ELK Stack); las de **monitorización de red** (Wireshark, Nagios, Zabbix) y las de **registro y auditoría** del sistema (Auditd en Linux, el Visor de eventos en Windows).

3 Buenas prácticas

1. **Define qué registrar:** no todo es relevante; prioriza accesos, cambios de configuración y errores de autenticación.
2. **Protege los registros:** guárdalos en un lugar seguro, sin que se puedan modificar ni borrar sin autorización.
3. **Revísalos con regularidad** y automatiza el análisis para localizar antes lo sospechoso.
4. **Configura alertas automáticas** ante eventos críticos (muchos intentos fallidos, accesos no autorizados, cambios de configuración).
5. **Ten un plan de respuesta a incidentes:** contener, investigar y resolver.
6. **Conserva los registros el tiempo que exija la normativa** y mantenlos accesibles para auditorías; haz además auditorías periódicas.

! DATO ACTUALIZADO

El temario cita la «LOPD», una referencia desfasada. Hoy rigen el RGPD/GDPR y la ley orgánica española que lo complementa; comprueba la normativa vigente en el BOE y en la AEPD, incluidos los plazos de conservación aplicables.

4 Dos casos prácticos

CASO 1 · ACCESOS FALLIDOS

Los logs de autenticación muestran muchos intentos fallidos desde una IP externa. Salta una alerta y se investiga un posible ataque de fuerza bruta.

CASO 2 · ARCHIVO ALTERADO

El monitor detecta un cambio no autorizado en un archivo crítico. Los logs revelan que lo hizo un usuario con privilegios elevados sin permiso para ello: posible ataque interno.

UNIDAD XXXVIII

Herramientas de ciberseguridad: código abierto y comerciales

Las herramientas de seguridad ayudan a detectar vulnerabilidades, vigilar el tráfico de red, auditar infraestructuras y responder a incidentes. Se dividen en dos grandes grupos: las de **código abierto** (el código está disponible para usarlo, modificarlo y distribuirlo) y las **comerciales** (requieren licencia o suscripción y suelen incluir soporte técnico).

1 Ejemplos por función

Función	Código abierto (ejemplos)	Comerciales (ejemplos)
Análisis de tráfico de red	Wireshark: captura y examina paquetes en tiempo real.	Plataformas de cortafuegos de nueva generación (NGFW), con inspección de aplicaciones.
Exploración y auditoría de red	Nmap: descubre equipos y servicios disponibles.	Suites de auditoría de pago.
Detección de intrusiones	Snort (IDS): busca patrones de actividad maliciosa, como escaneos de puertos o denegación de servicio.	Plataformas en la nube que usan inteligencia artificial para detectar amenazas (por ejemplo, CrowdStrike Falcon).
Escaneo de vulnerabilidades	OpenVAS: detecta fallos en redes y aplicaciones.	Escáneres con soporte profesional.
Pruebas de penetración	Metasploit Framework: herramienta de auditores para comprobar si una vulnerabilidad es explotable; requiere conocimientos avanzados y autorización.	Servicios de pentesting profesionales.

Función	Código abierto (ejemplos)	Comerciales (ejemplos)
Protección de equipos y SIEM	Graylog, ELK Stack.	Antivirus y protección de endpoints (Symantec, McAfee) y SIEM como SolarWinds SEM.

2 Código abierto frente a comercial

Aspecto	Código abierto	Comercial
Coste	Gratuitas o de bajo coste.	Normalmente caras.
Flexibilidad	Alta, porque se pueden modificar.	Limitada a lo que ofrece el proveedor.
Soporte	Comunidad de usuarios y foros.	Soporte técnico profesional.
Actualizaciones	Dependen de la comunidad.	Automáticas y garantizadas.
Facilidad de uso	Suelen exigir más conocimientos y tiempo de configuración.	Interfaces más sencillas.

3 Cómo elegir

- **Necesidad de seguridad:** qué amenazas quieres prevenir o detectar.
- **Tamaño de la infraestructura:** hay herramientas pensadas para grandes empresas y otras para pymes.
- **Presupuesto:** el código abierto ahorra licencias; lo comercial aporta funciones avanzadas a cambio de inversión.
- **Capacidad técnica del equipo** para implantarla y mantenerla.

Una combinación bien pensada de ambas categorías suele dar la protección más completa.

UNIDAD XXXIX

Contraseñas seguras y gestores de contraseñas

La contraseña es la primera línea de defensa de tus cuentas. Las débiles están entre las causas principales de brechas, porque se adivinan con ataques automáticos de **diccionario** (probar palabras y combinaciones habituales) o de **fuerza bruta** (probar todas las combinaciones posibles). Protegen tus datos personales, frenan el acceso a redes corporativas y, según el temario, normas como el GDPR o PCI-DSS las exigen.

1 Cómo es una contraseña segura

- **Larga:** al menos 12-16 caracteres. Cuanto más larga, más cuesta adivinarla.
- **Compleja:** mezcla mayúsculas, minúsculas, números y símbolos.

- **Impredecible:** sin nombres, fechas de nacimiento ni claves típicas como «123456» o «contraseña»; los atacantes usan listas de contraseñas comunes.
- **Única:** si repites contraseña y una cuenta cae, caen todas.
- **Mejor como frase:** una frase larga y fácil de recordar cumple longitud y complejidad.

CORREGIDO

El temario propone como ejemplo «MiGato@Rojo2024!», que sigue un patrón muy previsible (nombre + símbolo + año). Es mejor una frase larga y poco habitual o una clave aleatoria generada por un gestor.

2 Errores comunes

- Contraseñas cortas o simples como «12345» o «abcde»: se adivinan en segundos.
- Reutilizar la misma contraseña en varias cuentas.
- Basarlas en información personal (familiares, fechas, mascota).
- No cambiarlas nunca, ni siquiera cuando se sospecha que están comprometidas.

DATO ACTUALIZADO

El temario recomienda cambiar las contraseñas periódicamente. Hoy se insiste sobre todo en cambiarlas **siempre que haya sospecha de compromiso** y en que sean largas y únicas; comprueba las recomendaciones vigentes de organismos como INCIBE.

3 Gestores de contraseñas

Un **gestor de contraseñas** es una herramienta que genera, almacena cifradas y rellena tus contraseñas, de modo que solo necesitas recordar una clave maestra. Ejemplos: Bitwarden (código abierto), 1Password, Dashlane o LastPass.

GENERACIÓN

Crea contraseñas aleatorias y complejas para cada cuenta.

ALMACENAMIENTO CIFRADO

Las guarda cifradas, de modo que siguen protegidas aunque el dispositivo o la base de datos se vea comprometida.

ACCESO Y SINCRONIZACIÓN

Las tienes disponibles en ordenador, móvil y tableta sin memorizarlas.

Al elegir uno, comprueba que use **cifrado fuerte** (por ejemplo, AES-256), admita **MFA**, incluya generador de contraseñas y funcione en todos tus dispositivos. Protege la clave maestra como lo más valioso que tienes.

4 Buenas prácticas de gestión

- No compartas contraseñas por correo, mensajes ni otros medios inseguros.
- Activa la autenticación multifactor siempre que puedas.
- Revisa periódicamente los ajustes de seguridad de tus cuentas por si hay intentos de acceso no autorizados.

UNIDAD XL

Consejos para una vida digital segura (personal y profesional)

La seguridad no depende solo de software: también de los hábitos diarios. Todo se apoya en tres principios: **confidencialidad** (mantener privados los datos personales, familiares y profesionales), **integridad** (que la información no se altere ni destruya sin autorización) y **disponibilidad** (que esté accesible para quien debe usarla cuando la necesite).

1 Seguridad personal

ACCESO

Contraseñas fuertes y únicas, gestor de contraseñas y MFA en todas las cuentas que lo permitan.

NAVEGACIÓN

Comprueba que la web usa HTTPS y es legítima, no pulses enlaces sospechosos (típico del phishing) y usa VPN en redes públicas.

DISPOSITIVOS

Mantén el software actualizado, usa un antivirus fiable y cifra el disco (por ejemplo, BitLocker o FileVault) para que, si pierdes el equipo, nadie pueda leer los datos sin la clave.

COPIAS DE SEGURIDAD

Haz copias en la nube o en discos externos y comprueba de vez en cuando que sabes restaurarlas.

2 Seguridad profesional

- **Información confidencial:** no compartas contraseñas con compañeros, cifra el correo con información sensible (S/MIME o PGP) y limita los accesos a lo que cada puesto necesita (mínimo privilegio).
- **Formación:** talleres periódicos sobre phishing, contraseñas y políticas de seguridad, y simulacros de phishing para medir la preparación del personal.
- **Dispositivos:** móviles y tabletas con contraseña, cifrado y bloqueo (PIN o biometría); si se permite BYOD (usar dispositivos personales), con políticas de seguridad que los gestionen.
- **Detección y respuesta:** monitorización constante y procedimientos claros para responder rápido a cualquier incidente (ver la unidad sobre monitorización).

3 Gestión de la información

- **Clasifica** los datos en personales, confidenciales y públicos, con etiquetas o un sistema de clasificación.
- **Elimina de forma segura** lo que ya no necesites.
- **Redes sociales:** no publiques datos personales ni detalles laborales sensibles que sirvan para ingeniería social, y revisa la privacidad de tus perfiles.

4 Teletrabajo

- Conéctate con VPN desde casa o desde lugares públicos y evita el Wi-Fi público para tareas importantes.
- Separa trabajo y vida personal: si puedes, usa equipos distintos.
- Guarda los documentos de trabajo en el almacenamiento corporativo en la nube, con acceso controlado.

! RECUERDA

La seguridad se construye con herramientas bien configuradas y con hábitos conscientes: actualiza, limita permisos, usa contraseñas únicas con gestor y MFA, y vigila los registros. La formación continua es lo que mantiene todo eso en pie.

Datos clave para el examen del curso de Ciberseguridad y seguridad informática

Un repaso rápido de los datos del manual que más se preguntan:

3 principios
de la tríada CIA: confidencialidad, integridad y disponibilidad

Riesgo
probabilidad × impacto: la amenaza explota una vulnerabilidad

4 pasos
de la gestión del riesgo: identificar, analizar, tratar y dar seguimiento

4 tipos
de cortafuegos: filtrado de paquetes, con estado, de aplicación y de nueva generación

TLS 1.2 o 1.3
versiones recomendadas para el cifrado en tránsito

3 factores
de autenticación: algo que sabes, que tienes y que eres (mínimo dos distintos)

12+ caracteres
longitud mínima orientativa de una contraseña segura

3-2-1
3 copias de seguridad, 2 tipos de medio y 1 fuera del sitio

5 fases
de respuesta a incidentes: detección, contención, erradicación, recuperación y lecciones aprendidas

72 horas
para notificar una brecha de datos personales, según el temario

SaaS · PaaS · IaaS
modelos de nube: aplicación, plataforma e infraestructura

4 niveles
de clasificación de la información: público, interno, confidencial y secreto

¿Has terminado el manual?

Haz ahora el examen y, si lo apruebas, podrás obtener tu certificado.

academia-formacion.com/examen-ciberseguridad-%c2%b7-seguridad-informatica/