Ciberseguridad y regulación

¿Alguna vez te ha llegado un correo que dice «tu paquete te está esperando, haz clic aquí para pagar la tasa de aduanas»? ¿O un mensaje de «tu banco» que te pide que confirmes la contraseña? Ahora imagina que quien hace clic no eres tú, sino el recepcionista de un hotel, y que el ordenador que hay detrás de ese clic guarda los pasaportes de todos los clientes de la temporada.

Todas las empresas que has estudiado este curso dependen de sus datos: reservas, pedidos, lecturas de contadores, historiales de pacientes. En el juego de construir ciudades, todas esas vistas de información no valen nada si cualquiera puede entrar en el ayuntamiento y cambiar los registros, o apagar la central eléctrica. La ciberseguridad es la policía, las murallas y las cerraduras de la ciudad. Y, como en una ciudad real, hay leyes que dicen qué cerraduras son obligatorias. Esta lección trata de las dos cosas, y tú mismo comprobarás las cerraduras de una web real, desde fuera, sin tocar nada.

Qué aprenderás

- Explicar qué protege la seguridad: **confidencialidad**, **integridad** y **disponibilidad**
- Clasificar las medidas de seguridad en nivel de **dispositivo**, de **sistema** y **global**
- Hacer una revisión de seguridad **pasiva** de una web pública: cabeceras de seguridad, cookies antes del consentimiento y política de privacidad
- Comprobar si tu propio correo electrónico aparece en una **brecha de datos** conocida
- Explicar qué regulan el **RGPD**, la **LOPDGDD** y **NIS2**, y decidir si cada uno se aplica a una empresa
- Evitar la trampa: proteger cada portátil no basta si no hay una copia de seguridad probada

Qué protegemos: confidencialidad, integridad, disponibilidad

> La **seguridad de la información** protege la información en cualquier forma, incluidos el papel y las personas. La **ciberseguridad** es la parte que protege las redes, los sistemas y los datos digitales frente a ataques e incidentes.

Las dos protegen las mismas tres cosas, que se suelen llamar la **tríada CID** (en inglés, *CIA triad*):

Pilar	Qué garantiza	Se rompe cuando…	En la ciudad
Confidencialidad	Solo las personas autorizadas pueden acceder a los datos	Se filtra una base de datos de clientes	Desconocidos leyendo los archivos del ayuntamiento
Integridad	Los datos son correctos y nadie los ha cambiado sin permiso	Alguien altera precios o notas	Alguien falsificando el registro de la propiedad
Disponibilidad	Los datos y los sistemas funcionan cuando hacen falta	Un ataque o un fallo tumba el servicio	La central eléctrica apagada

Recuerda la lección de la Unidad 1 sobre IT y OT: en OT (la planta, las bombas, las máquinas) la **disponibilidad** y la seguridad física suelen ir primero, porque una planta de agua parada es peor que una hoja de cálculo filtrada. En la IT de oficina, la confidencialidad suele recibir más atención. Es una regla general, no una ley.

Tres niveles de seguridad

Nivel	Alcance	Medidas típicas	En la ciudad
Dispositivo	Cada dispositivo: ordenador, móvil, servidor, sensor	Actualizaciones, antimalware, cifrado del disco, bloqueo de pantalla, contraseñas robustas y **autenticación de doble factor** (una segunda prueba, como un código en el móvil)	Una cerradura en cada puerta
Sistema	Toda la organización: red, aplicaciones, personas, procesos	Cortafuegos y segmentación de la red, mínimo privilegio, copias de seguridad **probadas**, monitorización, un plan de respuesta a incidentes, formación del personal	La policía, las murallas, el plan de los bomberos
Global	Sectores, países y la cadena de suministro	Leyes y directivas, normas, equipos públicos de respuesta a incidentes, cooperación internacional, requisitos de seguridad para los proveedores	Las leyes del país y la cooperación entre ciudades

Ejemplos del nivel global: **ENISA**, la Agencia de la Unión Europea para la Ciberseguridad, y en España **INCIBE**, el Instituto Nacional de Ciberseguridad, cuya línea de ayuda gratuita y confidencial **017** atiende a ciudadanos, empresas y profesionales.

> **Cuidado: el nivel de dispositivo no basta**
> Un portátil perfectamente protegido no salva a una empresa sin copias de seguridad. Un cortafuegos no impide que un empleado escriba su contraseña en una página falsa. El **factor humano** (el **phishing**: mensajes falsos que te engañan para que hagas clic o des tus credenciales) atraviesa los tres niveles. La seguridad es un sistema, no un producto.

En clase: una revisión de seguridad pasiva de una web real

Mirarás la web pública de la empresa de tu proyecto igual que lo hace el navegador de cualquier visitante, y nada más.

> **Solo pasiva**
> Solo **miras** lo que la web ya muestra a cualquier visitante: sus cabeceras de respuesta, las cookies que guarda en tu propio navegador, su aviso de cookies y su política de privacidad. **Nunca** escanees puertos, pruebes contraseñas, pruebes formularios con entradas extrañas ni uses ninguna herramienta de «hacking» contra una empresa real. Hacerlo sin permiso por escrito puede ser delito según el Código Penal. Las dos herramientas en línea de abajo solo hacen una visita normal a la página de inicio, como hace tu navegador.

Trabaja de forma **individual**. **Sin herramientas de IA.**

Paso	Haz esto	Deberías ver
1 · HTTPS	Abre la web de la empresa. Haz clic en el icono a la izquierda de la dirección y mira el certificado: ¿quién lo emitió y hasta cuándo es válido?	Un candado o «la conexión es segura», un emisor y una fecha de caducidad
2 · Cabeceras	Ve a securityheaders.com, pega la dirección y analízala. Anota la nota y qué cabeceras **faltan**.	Una nota de A+ a F y una lista en rojo y verde
3 · Observatory	Haz lo mismo en Mozilla HTTP Observatory. Anota la puntuación y las dos pruebas fallidas más importantes.	Una puntuación y una lista de pruebas
4 · Cookies antes del consentimiento	Abre una **ventana privada**, abre DevTools (`F12`) → *Application* (*Storage* en Firefox) → *Cookies*, y carga la web. **No hagas clic en el aviso.** Haz una lista de las cookies que ya se han guardado. Después haz clic en *Rechazar* y recarga: ¿se ha quedado alguna cookie de analítica o de publicidad (nombres como `_ga`, `_fbp`)?	Una lista de cookies con sus dominios
5 · Aviso	¿Hay aviso de cookies? ¿*Rechazar* es tan fácil como *Aceptar* (mismo nivel, mismo tamaño)?	Sí o no, con una captura de pantalla
6 · Política de privacidad	En la política de privacidad, busca: quién es el responsable, el contacto del delegado de protección de datos (si lo hay), las finalidades, los plazos de conservación, los derechos y cómo ejercerlos, y el derecho a reclamar ante la AEPD.	Una lista de comprobación con encontrado / no encontrado
7	Entrega la ficha de auditoría en Classroom: URL, fecha y hora, capturas de pantalla y una tabla de hallazgos con una medida recomendada para cada uno.	

Qué hacen las cabeceras más habituales:

Cabecera	Qué hace, en una línea
`Strict-Transport-Security` (HSTS)	Indica al navegador que use siempre HTTPS con esta web
`Content-Security-Policy` (CSP)	Indica desde dónde se pueden cargar scripts y otros contenidos, lo que limita los scripts inyectados
`X-Frame-Options`	Impide que otras webs muestren esta dentro de un marco para engañar con los clics
`X-Content-Type-Options`	Impide que el navegador adivine los tipos de archivo (`nosniff`)
`Referrer-Policy`	Controla cuánto de la dirección se envía a otras webs cuando haces clic en un enlace
`Permissions-Policy`	Desactiva funciones del navegador que la web no necesita (cámara, micrófono, ubicación)

Una mala nota es un hallazgo, no una prueba de que hayan atacado la web. Escribe los hallazgos con educación y con pruebas: «el 26/04/2027 a las 10:15 la web no enviaba `Content-Security-Policy`».

Tu propio correo: Have I Been Pwned

Have I Been Pwned es un servicio gratuito que gestiona desde 2013 el investigador de seguridad Troy Hunt. Recopila las listas de cuentas de brechas de datos conocidas y te permite comprobar si **tu propia** dirección de correo aparece en ellas. Solo pide el correo, **nunca** una contraseña.

Comprueba tu propia dirección (solo la tuya). Si aparece: cambia la contraseña de ese servicio y de cualquier otro en el que la hayas reutilizado, usa una contraseña distinta para cada web (un gestor de contraseñas ayuda) y activa la autenticación de doble factor. **No** entregues tu resultado: es un dato personal. En la actividad de Classroom responde solo «¿qué haría una empresa si el correo de un empleado apareciera en una brecha?».

Las leyes: RGPD, LOPDGDD y NIS2

	RGPD (GDPR en inglés)	LOPDGDD	NIS2
Nombre oficial	Reglamento (UE) 2016/679	*Ley Orgánica 3/2018*, de 5 de diciembre	Directiva (UE) 2022/2555
Tipo	Reglamento de la UE: se aplica directamente en todos los Estados miembros, desde el 25 de mayo de 2018	Ley orgánica española, en vigor desde el 7 de diciembre de 2018	Directiva de la UE: cada Estado debe **transponerla** a su propia legislación; plazo, el 17 de octubre de 2024
Protege	A las personas, en cuanto al tratamiento de sus **datos personales**	Lo mismo: adapta y completa el RGPD en España y añade **derechos digitales** (por ejemplo, la desconexión digital en el trabajo)	Las **redes y sistemas de información** de los sectores clave
A quién obliga	A cualquiera que trate datos personales de personas en la UE, sea cual sea su tamaño	Los tratamientos sujetos a la ley española	**Entidades esenciales** e **importantes** de los sectores de sus anexos, normalmente a partir de tamaño mediano
Ideas clave	Principios, base jurídica, derechos, privacidad desde el diseño, notificación de brechas en 72 horas	La autoridad es la **AEPD** (*Agencia Española de Protección de Datos*)	Gestión de riesgos, notificación de incidentes (alerta temprana en 24 h, notificación en 72 h, informe final en un mes), responsabilidad de la dirección, seguridad de la cadena de suministro
Multas máximas	Hasta 20 millones de euros o el 4 % del volumen de negocio anual mundial, la cifra más alta	Clasifica las infracciones del RGPD en muy graves, graves o leves	Hasta 10 millones de euros o el 2 % del volumen de negocio para las entidades esenciales; 7 millones de euros o el 1,4 % para las importantes

RGPD: lo que necesita saber un desarrollador

- **Datos personales**: cualquier información sobre una persona identificada o identificable: nombre, correo electrónico, DNI, dirección IP, ubicación. Las **categorías especiales** (salud, datos biométricos y genéticos, opiniones políticas, religión, origen étnico, orientación sexual…) tienen una protección adicional.
- **Principios**: licitud, lealtad y transparencia; limitación de la finalidad; **minimización de datos** (recoge solo lo que necesitas); exactitud; limitación del plazo de conservación (la etapa de eliminación del ciclo de vida); integridad y confidencialidad; responsabilidad proactiva.
- **Derechos**: acceso, rectificación, supresión, limitación, portabilidad y oposición.
- **Roles**: el **responsable del tratamiento** decide para qué son los datos; el **encargado del tratamiento** los trata por cuenta del responsable (un proveedor de nube, una empresa de software).
- **Privacidad desde el diseño y por defecto**: la privacidad se planifica cuando se diseña la aplicación, no se parchea al final.

- **Brechas**: una brecha de datos personales se debe notificar a la AEPD sin dilación indebida y, si es posible, en un plazo de **72 horas**, salvo que sea improbable que suponga un riesgo para las personas.

Las cookies tienen su propia norma española: el artículo 22.2 de la ley de servicios de la sociedad de la información (*Ley 34/2002*, LSSI) exige un consentimiento informado antes de guardar cookies que no sean estrictamente necesarias. La guía de cookies de la AEPD (actualizada en mayo de 2024) añade que rechazar debe ser tan fácil como aceptar. Es lo que has comprobado en los pasos 4 y 5.

NIS2 en España

NIS2 sustituyó a la primera directiva NIS (2016/1148). A octubre de 2026, **España todavía no la ha transpuesto**: el Gobierno aprobó el anteproyecto de *Ley de Coordinación y Gobernanza de la Ciberseguridad* el 14 de enero de 2025, y el 8 de julio de 2026 la Comisión Europea llevó a España (junto con Irlanda, Francia y los Países Bajos) ante el Tribunal de Justicia de la UE por no transponerla. Mientras tanto, sigue en vigor el *Real Decreto-ley 12/2018*, que transpuso la primera directiva NIS. **Consulta el BOE** cuando escribas tu entrega: esto puede haber cambiado.

¿Se aplica a mi empresa?

Pregunta	Si la respuesta es sí
¿La empresa trata datos personales de personas en la UE (clientes, empleados, pacientes)?	Se aplican el **RGPD** y, en España, la **LOPDGDD**. Casi todas las empresas responden que sí.
¿Su web usa cookies que no son estrictamente necesarias?	Artículo 22.2 de la **LSSI**: primero, el consentimiento
¿Está en un sector del anexo I de NIS2? Energía, transporte (aéreo, ferroviario, marítimo, por carretera; puertos y aeropuertos), banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, infraestructura digital, gestión de servicios TIC, administración pública, espacio	Posible **entidad esencial** (si es grande) o **importante**
¿Está en un sector del anexo II? Servicios postales, gestión de residuos, sustancias químicas, alimentación (producción industrial, transformación y distribución al por mayor), fabricación de algunos productos, proveedores digitales, investigación	Posible **entidad importante**
¿Es al menos mediana: 50 empleados o más, o un volumen de negocio anual y un balance de más de 10 millones de euros?	Necesario, en general, para que se aplique NIS2; las empresas más pequeñas pueden verse afectadas igualmente como **proveedoras** de una entidad incluida

Una cadena hotelera: RGPD y LOPDGDD, sí; el turismo no es un sector de NIS2. Una empresa de agua: RGPD y LOPDGDD, sí, y el agua potable está en el anexo I de NIS2.

Para tu proyecto

La auditoría pasiva es la **sección D** de la Entrega 5 (la sección del cuarto miembro). La pregunta «cuáles de RGPD, LOPDGDD y NIS2 se aplican, y por qué» es la **parte de grupo**, junto con la tabla de riesgos: cada riesgo, qué pilar de la tríada amenaza, su nivel y la medida que lo reduce.

Ideas clave

- La seguridad protege la **confidencialidad**, la **integridad** y la **disponibilidad** (la tríada CID).
- Las medidas actúan a nivel de **dispositivo**, de **sistema** y **global**; el factor humano (el **phishing**) atraviesa los tres.
- Una auditoría **pasiva** solo mira lo que ve cualquier visitante: cabeceras, cookies, aviso, política de privacidad. Nunca escanees ni pruebes accesos en una empresa real.
- El **RGPD** (Reglamento (UE) 2016/679) y la **LOPDGDD** (Ley Orgánica 3/2018) protegen los datos personales de las personas; **NIS2** (Directiva (UE) 2022/2555) protege las redes y los sistemas de los sectores clave.
- A octubre de 2026 España no ha transpuesto NIS2; sigue en vigor el Real Decreto-ley 12/2018.
- Las cookies que no son estrictamente necesarias necesitan primero el consentimiento (artículo 22.2 de la LSSI).

Comprobación rápida

1 Un ataque de denegación de servicio deja la web de reservas fuera de línea durante un día. ¿Qué pilar recibe el golpe más fuerte?

A Confidencialidad
B Integridad
C Disponibilidad
D Ninguno: no se ha robado ningún dato

2 Cifrar el disco de un portátil, ¿es una medida de qué nivel?

A Dispositivo
B Sistema
C Global
D Ninguno: el cifrado no es una medida de seguridad

3 ¿Cuál de estas acciones está permitida en la actividad de seguridad de este curso?

A Escanear los puertos del servidor de la empresa para ver qué hay abierto
B Probar contraseñas comunes en la página de acceso del personal
C Leer las cabeceras de respuesta y las cookies que la web guarda en tu propio navegador
D Enviar entradas extrañas al formulario de contacto para ver si se rompe

4 ¿Qué norma se aplica directamente en todos los Estados de la UE sin necesidad de transposición?

A El RGPD, Reglamento (UE) 2016/679
B NIS2, Directiva (UE) 2022/2555
C La LOPDGDD, Ley Orgánica 3/2018
D El Real Decreto-ley 12/2018

5 Una app de reservas pide la fecha de nacimiento, el DNI y las alergias alimentarias solo para reservar una mesa. ¿Qué principio del RGPD incumple de forma más clara?

A Portabilidad
B Minimización de datos
C Exactitud
D Disponibilidad

6 Al cargar una web en una ventana privada, antes de tocar el aviso, DevTools ya muestra una cookie de analítica `_ga`. ¿Qué sugiere?

- **A** Nada: todas las cookies están permitidas hasta que haces clic
- **B** Puede que se haya guardado una cookie no estrictamente necesaria antes del consentimiento, algo que el artículo 22.2 de la LSSI no permite
- **C** Han atacado la web
- **D** El RGPD no cubre las webs

7 La empresa de tu proyecto es una compañía mediana de agua potable de Mallorca con un área de clientes en línea. Elige las dos afirmaciones verdaderas.

- **A** Se aplican el RGPD y la LOPDGDD, porque trata datos personales de los clientes
- **B** Solo se aplica NIS2, porque el agua es una infraestructura
- **C** El agua potable es un sector del anexo I de NIS2, así que probablemente será una entidad sujeta a NIS2 cuando España la transponga
- **D** No se aplica ninguna ley hasta que España transponga NIS2

Ya has recorrido toda la unidad. Júntalo todo para tu empresa en la Entrega 5 · Informe de datos y seguridad.

Soluciones

1. C · Nadie ha leído ni cambiado los datos, pero el servicio no funcionaba cuando hacía falta. Eso es **disponibilidad**.

2. A · Protege **un dispositivo**. La segmentación de la red o las copias de seguridad probadas para toda la empresa serían del nivel de **sistema**.

3. C · Solo comprobaciones **pasivas**: mirar lo que la web ya muestra a cualquier visitante. Las otras tres sondean los sistemas de la empresa sin permiso.

4. A · Un **reglamento** de la UE se aplica directamente. Una **directiva** como NIS2 la tiene que transponer cada Estado, y la LOPDGDD y el real decreto-ley son normas españolas.

5. B · **Minimización de datos**: recoge solo lo que necesita la finalidad. Una alergia, además, es un dato de salud, una categoría especial.

6. B · Las cookies de analítica no son estrictamente necesarias, así que el consentimiento debería ir **primero**. Es un hallazgo que hay que comunicar con educación y con pruebas, no una prueba de un ataque.

7. A, C · Las leyes **se suman**: los datos personales traen el **RGPD** y la **LOPDGDD**, y el sector y el tamaño traen **NIS2**. El RGPD se aplica hoy, con independencia de la transposición de NIS2.