Ciberseguretat i regulació

Alguna vegada has rebut un correu que diu “el teu paquet t’espera, fes clic aquí per pagar les taxes de duana”? O un missatge del “teu banc” que et demana que confirmis la contrasenya? Ara imagina que qui fa clic no ets tu, sinó el recepcionista d’un hotel, i que l’ordinador que hi ha darrere del clic guarda els passaports de tots els clients de la temporada.

Totes les empreses que has estudiat aquest curs depenen de les seves dades: reserves, comandes, lectures de comptadors, historials de pacients. Al joc de construir ciutats, totes aquestes vistes d’informació no valen res si qualsevol pot entrar a l’ajuntament i canviar els registres, o apagar la central elèctrica. La ciberseguretat és la policia, les murades i els panys de la ciutat. I, com en una ciutat real, hi ha lleis que diuen quins panys són obligatoris. Aquesta lliçó tracta totes dues coses, i comprovaràs tu mateix els panys d’un lloc web real, des de fora, sense tocar res.

Què aprendràs

- Explicar què protegeix la seguretat: la **confidencialitat**, la **integritat** i la **disponibilitat**
- Classificar les mesures de seguretat en nivell de **dispositiu**, de **sistema** i **global**
- Fer una comprovació de seguretat **passiva** d’un lloc web públic: capçaleres de seguretat, galetes abans del consentiment i la política de privadesa
- Comprovar si la teva adreça de correu surt en alguna **bretxa de dades** coneguda
- Explicar què regulen el **RGPD**, la **LOPDGDD** i la **NIS2**, i decidir si cada un s’aplica a una empresa
- Evitar la trampa: protegir tots els portàtils no basta si no hi ha una còpia de seguretat provada

Què protegim: confidencialitat, integritat, disponibilitat

> La **seguretat de la informació** protegeix la informació en qualsevol forma, incloent-hi el paper i les persones. La **ciberseguretat** és la part que protegeix les xarxes, els sistemes i les dades digitals contra atacs i incidents.

Totes dues protegeixen les mateixes tres coses, sovint anomenades la **tríada CID** (en anglès, *CIA triad*):

Pilar	Què garanteix	Es trenca quan…	A la ciutat
Confidencialitat	Només les persones autoritzades poden accedir a les dades	Es filtra una base de dades de clients	Desconeguts que llegeixen els expedients de l’ajuntament
Integritat	Les dades són correctes i ningú no les ha canviades sense permís	Algú altera preus o notes	Algú que falsifica el registre de la propietat

Pilar	Què garanteix	Es trenca quan...	A la ciutat
Disponibilitat	Les dades i els sistemes funcionen quan es necessiten	Un atac o una avaria fa caure el servei	La central elèctrica apagada

Recorda la lliçó de la Unitat 1 sobre IT i OT: a l'OT (la planta, les bombes, les màquines) la **disponibilitat** i la seguretat física solen anar primer, perquè una potabilitzadora aturada és pitjor que un full de càlcul filtrat. A la IT d'oficina, la confidencialitat sol rebre més atenció. És una regla general, no una llei.

Tres nivells de seguretat

Nivell	Abast	Mesures típiques	A la ciutat
Dispositiu	Cada dispositiu: ordinador, mòbil, servidor, sensor	Actualitzacions, antimalware, xifratge del disc, bloqueig de pantalla, contrasenyes fortes i **autenticació de doble factor** (una segona prova, com un codi al mòbil)	Un pany a cada porta
Sistema	Tota l'organització: xarxa, aplicacions, persones, processos	Tallafoc i segmentació de la xarxa, privilegi mínim, còpies de seguretat **provades**, monitoratge, un pla de resposta a incidents, formació del personal	La policia, les muralles, el pla dels bombers
Global	Sectors, països i la cadena de subministrament	Lleis i directives, estàndards, equips públics de resposta a incidents, cooperació internacional, requisits de seguretat per als proveïdors	Les lleis del país i la cooperació entre ciutats

Exemples del nivell global: l'**ENISA**, l'Agència de la Unió Europea per a la Ciberseguretat, i a Espanya l'**INCIBE**, l'Institut Nacional de Ciberseguretat, que té la línia d'ajuda gratuïta i confidencial **017** per a ciutadans, empreses i professionals.

> **Compte: el nivell de dispositiu no basta**
> Un portàtil perfectament protegit no salva una empresa sense còpies de seguretat. Un tallafoc no impedeix que un treballador escrigui la contrasenya en una pàgina falsa. El **factor humà** (la **pesca electrònica** o ***phishing***: missatges falsos que t'enganyen perquè facis clic o donis les teves credencials) travessa els tres nivells. La seguretat és un sistema, no un producte.

A classe: una comprovació de seguretat passiva d'un lloc web real

Miraràs el lloc web públic de l'empresa del teu projecte tal com ho fa el navegador de qualsevol visitant, i res més.

> **Només passiva**
> Només **mires** el que el lloc web ja mostra a qualsevol visitant: les capçaleres de resposta, les galetes que posa al teu propi navegador, el bàner de galetes i la política de privadesa. **Mai** no escanegis ports, no provis contrasenyes, no posis dades estranyes als formularis ni facis servir cap eina de "hacking" contra una empresa real. Fer-ho sense

> permís per escrit pot ser delicte segons el Codi Penal espanyol. Les dues eines en línia que tens a continuació només fan una visita normal a la pàgina d'inici, com el teu navegador.

Treballa **individualment**. **Cap eina d'IA.**

Pas	Fes això	Hauries de veure
1 · HTTPS	Obre el lloc web de l'empresa. Fes clic a la icona de l'esquerra de l'adreça i mira el certificat: qui l'ha emès i fins quan és vàlid?	Un cadenat o "connexió segura", un emissor i una data de caducitat
2 · Capçaleres	Ves a securityheaders.com, enganxa l'adreça i fes l'escaneig. Apunta la nota i quines capçaleres **falten**.	Una nota de l'A+ a la F i una llista en vermell i verd
3 · Observatory	Fes el mateix a Mozilla HTTP Observatory. Apunta la puntuació i les dues proves fallides més importants.	Una puntuació i una llista de proves
4 · Galetes abans del consentiment	Obre una **finestra privada**, obre DevTools (`F12`) → *Application* (*Storage* al Firefox) → *Cookies*, i carrega el lloc. **No facis clic al bàner.** Fes la llista de les galetes que ja s'han posat. Després fes clic a *Rebutjar* i torna a carregar: s'hi ha quedat alguna galeta d'analítica o de publicitat (noms com `_ga`, `_fbp`)?	Una llista de galetes amb els seus dominis
5 · Bàner	Hi ha bàner de galetes? *Rebutjar* és tan fàcil com *Acceptar* (al mateix nivell, de la mateixa mida)?	Sí o no, amb una captura de pantalla
6 · Política de privadesa	A la política de privadesa, cerca: qui n'és el responsable, el contacte del delegat de protecció de dades (si n'hi ha), les finalitats, els terminis de conservació, els drets i com exercir-los, i el dret a presentar una reclamació a l'AEPD.	Una llista de comprovació amb trobat / no trobat
7	Lliura el full d'auditoria a Classroom: URL, data i hora, captures de pantalla i una taula de troballes amb una mesura recomanada per a cada una.	

Què fan les capçaleres més habituals:

Capçalera	Què fa, en una línia
`Strict-Transport-Security` (HSTS)	Diu al navegador que faci servir sempre HTTPS per a aquest lloc
`Content-Security-Policy` (CSP)	Llista d'on es poden carregar els scripts i altres continguts, cosa que limita els scripts injectats
`X-Frame-Options`	Impedeix que altres llocs mostrin aquest dins un marc per enganyar els clics
`X-Content-Type-Options`	Impedeix que el navegador endevini el tipus dels fitxers (`nosniff`)
`Referrer-Policy`	Controla quina part de l'adreça s'envia a altres llocs quan fas clic en un enllaç
`Permissions-Policy`	Desactiva funcions del navegador que el lloc no necessita (càmera, micròfon, ubicació)

Una mala nota és una troballa, no la prova que el lloc hagi estat atacat. Escriu les troballes amb educació i amb evidències: "el 26/04/2027 a les 10:15 el lloc no enviava `Content-Security-Policy`".

El teu propi correu: Have I Been Pwned

Have I Been Pwned és un servei gratuït que gestiona des del 2013 l'investigador de seguretat Troy Hunt. Recull les llistes de comptes de bretxes de dades conegudes i et permet comprovar si **la teva** adreça de correu hi surt. Només et demana el correu, **mai** una contrasenya.

Comprova la teva adreça (només la teva). Si hi surt: canvia la contrasenya d'aquell servei i de qualsevol altre on l'hagis reutilitzada, fes servir una contrasenya diferent per a cada lloc (un gestor de contrasenyes t'hi ajuda) i activa l'autenticació de doble factor. **No** lliuris el resultat: és una dada personal. A l'activitat de Classroom només has de respondre "què faria una empresa si el correu d'un treballador sortís en una bretxa?".

Les lleis: RGPD, LOPDGDD i NIS2

	RGPD (GDPR en anglès)	LOPDGDD	NIS2
Nom oficial	Reglament (UE) 2016/679	*Ley Orgánica 3/2018*, de 5 de desembre	Directiva (UE) 2022/2555
Tipus	Reglament de la UE: s'aplica directament a tots els estats membres, des del 25 de maig de 2018	Llei orgànica espanyola, en vigor des del 7 de desembre de 2018	Directiva de la UE: cada estat l'ha de **transposar** a la seva pròpia llei; termini, 17 d'octubre de 2024
Protegeix	Les persones, pel que fa al tractament de les seves **dades personals**	El mateix: adapta i completa el RGPD a Espanya i hi afegeix **drets digitals** (per exemple, la desconnexió digital a la feina)	Les **xarxes i sistemes d'informació** dels sectors clau
A qui obliga	Qualsevol que tracti dades personals de persones de la UE, sigui de la mida que sigui	Els tractaments subjectes a la llei espanyola	Les entitats **essencials** i **importants** dels sectors dels seus annexos, normalment a partir de mida mitjana
Idees clau	Principis, base jurídica, drets, privadesa des del disseny, notificació de bretxes en 72 hores	L'autoritat és l'**AEPD** (*Agencia Española de Protección de Datos*)	Gestió de riscos, notificació d'incidents (alerta primerenca en 24 h, notificació en 72 h, informe final en un mes), responsabilitat de la direcció, seguretat de la cadena de subministrament
Multes màximes	Fins a 20 milions d'euros o el 4% del volum de negoci anual mundial, la xifra més alta	Classifica les infraccions del RGPD en molt greus, greus o lleus	Fins a 10 milions d'euros o el 2% del volum de negoci per a les entitats essencials; 7 milions d'euros o l'1,4% per a les importants

RGPD: el que ha de saber un desenvolupador

- **Dada personal**: qualsevol informació sobre una persona identificada o identificable: nom, correu, DNI, adreça IP, ubicació. Les **categories especials** (dades de salut, biomètriques i genètiques, opinions polítiques, religió, origen ètnic, orientació sexual...) tenen protecció addicional.
- **Principis**: licitud, lleialtat i transparència; limitació de la finalitat; **minimització de dades** (recollir només el que necessites); exactitud; limitació del termini de conservació (l'etapa d'eliminació del cicle de vida); integritat i confidencialitat; responsabilitat proactiva.
- **Drets**: accés, rectificació, supressió, limitació, portabilitat i oposició.
- **Rols**: el **responsable del tractament** decideix per a què són les dades; l'**encarregat del tractament** les tracta en nom del responsable (un proveïdor de núvol, una empresa de programari).

- **Privadesa des del disseny i per defecte**: la privadesa es planifica quan es dissenya l'aplicació, no s'hi posa un pedaç al final.
- **Bretxes**: una bretxa de dades personals s'ha de notificar a l'AEPD sense dilació indeguda i, si és possible, en un termini de **72 hores**, tret que sigui improbable que suposi un risc per a les persones.

Les galetes tenen la seva pròpia norma espanyola: l'article 22.2 de la llei de serveis de la societat de la informació (*Ley 34/2002*, LSSI) exigeix el consentiment informat abans de guardar galetes que no siguin estrictament necessàries. La guia de galetes de l'AEPD (actualitzada el maig de 2024) hi afegeix que rebutjar ha de ser tan fàcil com acceptar. Això és el que has comprovat als passos 4 i 5.

La NIS2 a Espanya

La NIS2 va substituir la primera directiva NIS (2016/1148). A l'octubre de 2026, **Espanya encara no l'ha transposada**: el govern va aprovar l'avantprojecte de *Ley de Coordinación y Gobernanza de la Ciberseguridad* el 14 de gener de 2025, i el 8 de juliol de 2026 la Comissió Europea va portar Espanya (amb Irlanda, França i els Països Baixos) davant el Tribunal de Justícia de la UE per no haver-la transposada. Mentrestant, continua en vigor el *Real Decreto-ley 12/2018*, que va transposar la primera directiva NIS. **Consulta el BOE** quan escriguis el lliurament: això pot haver canviat.

S'aplica a la meva empresa?

Pregunta	Si la resposta és sí
L'empresa tracta dades personals de persones de la UE (clients, treballadors, pacients)?	S'hi apliquen el **RGPD** i, a Espanya, la **LOPDGDD**. Gairebé totes les empreses responen que sí.
El seu lloc web fa servir galetes que no són estrictament necessàries?	Article 22.2 de la **LSSI**: primer, el consentiment
És d'un sector de l'annex I de la NIS2? Energia, transport (aeri, ferroviari, marítim, per carretera; ports i aeroports), banca, infraestructures dels mercats financers, salut, aigua potable, aigües residuals, infraestructura digital, gestió de serveis TIC, administració pública, espai	Possiblement entitat **essencial** (si és gran) o **important**
És d'un sector de l'annex II? Serveis postals, gestió de residus, productes químics, alimentació (producció industrial, transformació i distribució a l'engròs), fabricació d'alguns productes, proveïdors digitals, recerca	Possiblement entitat **important**
És almenys mitjana: 50 treballadors o més, o un volum de negoci anual i un balanç de més de 10 milions d'euros?	En general, cal perquè s'apliqui la NIS2; les empreses més petites també poden quedar afectades com a **proveïdores** d'una entitat que hi està inclosa

Una cadena hotelera: RGPD i LOPDGDD, sí; el turisme no és un sector de la NIS2. Una empresa d'aigües: RGPD i LOPDGDD, sí, i l'aigua potable és a l'annex I de la NIS2.

Per al teu projecte

L'auditoria passiva és l'**apartat D** del Lliurament 5 (l'apartat del quart membre). La pregunta "quines lleis s'apliquen entre RGPD, LOPDGDD i NIS2, i per què" és la **part de grup**, juntament amb la taula de riscos: cada risc, quin pilar de la tríada amenaça, el seu nivell i la mesura que el redueix.

Idees clau

- La seguretat protegeix la **confidencialitat**, la **integritat** i la **disponibilitat** (la tríada CID).
- Les mesures actuen a nivell de **dispositiu**, de **sistema** i **global**; el factor humà (la **pesca electrònica**) travessa els tres.
- Una auditoria **passiva** només mira el que veu qualsevol visitant: capçaleres, galetes, bàner, política de privadesa. Mai no escanegis ni provis inicis de sessió contra una empresa real.
- El **RGPD** (Reglament (UE) 2016/679) i la **LOPDGDD** (Ley Orgánica 3/2018) protegeixen les dades personals de les persones; la **NIS2** (Directiva (UE) 2022/2555) protegeix les xarxes i els sistemes dels sectors clau.
- A l'octubre de 2026 Espanya no ha transposat la NIS2; el Reial decret llei 12/2018 continua en vigor.
- Les galetes que no són estrictament necessàries necessiten primer el consentiment (article 22.2 de la LSSI).

Comprovació ràpida

1 Un atac de denegació de servei deixa el web de reserves fora de línia durant un dia. Quin pilar en surt més afectat?

A Confidencialitat
B Integritat
C Disponibilitat
D Cap: no s'han robat dades

2 Xifrar el disc d'un portàtil és una mesura de quin nivell?

A Dispositiu
B Sistema
C Global
D Cap: el xifratge no és una mesura de seguretat

3 Quina d'aquestes coses està permesa a l'activitat de seguretat d'aquest curs?

A Escanejar els ports del servidor de l'empresa per veure què hi ha obert
B Provar contrasenyes habituals a la pàgina d'inici de sessió del personal
C Llegir les capçaleres de resposta i les galetes que el lloc posa al teu propi navegador
D Enviar dades estranyes al formulari de contacte per veure si es trenca

4 Quina llei s'aplica directament a tots els estats de la UE sense haver de ser transposada?

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

5 Una aplicació de reserves demana la data de naixement, el DNI i les al·lèrgies alimentàries només per reservar una taula. Quin principi del RGPD incompleix més clarament?

A Portabilitat
B Minimització de dades
C Exactitud
D Disponibilitat

6 Quan carregues un lloc en una finestra privada, abans de tocar el bàner, DevTools ja mostra una galeta d'analítica `_ga`. Què indica?

- **A** Res: totes les galetes estan permeses fins que fas clic
- **B** Pot ser que s'hagi posat una galeta no estrictament necessària abans del consentiment, cosa que l'article 22.2 de la LSSI no permet
- **C** El lloc web ha estat atacat
- **D** El RGPD no cobreix els llocs web

7 L'empresa del teu projecte és una companyia mitjana d'aigua potable de Mallorca amb una àrea de clients en línia. Tria les dues afirmacions certes.

- **A** S'hi apliquen el RGPD i la LOPDGDD, perquè tracta dades personals dels clients
- **B** Només s'hi aplica la NIS2, perquè l'aigua és una infraestructura
- **C** L'aigua potable és un sector de l'annex I de la NIS2, així que probablement serà una entitat subjecta a la NIS2 quan Espanya la transposi
- **D** No s'hi aplica cap llei fins que Espanya transposi la NIS2

Ja has cobert tota la unitat. Posa-ho tot junt per a la teva empresa al Lliurament 5 · Informe de dades i seguretat.

Solucions

1. C · Ningú no ha llegit ni canviat les dades, però el servei no ha funcionat quan es necessitava. Això és la **disponibilitat**.

2. A · Protegeix **un dispositiu**. La segmentació de la xarxa o les còpies de seguretat provades de tota l'empresa serien de nivell de **sistema**.

3. C · Només comprovacions **passives**: mirar el que el lloc ja mostra a qualsevol visitant. Les altres tres sondegen els sistemes de l'empresa sense permís.

4. A · Un **reglament** de la UE s'aplica directament. Una **directiva** com la NIS2 l'ha de transposar cada estat, i la LOPDGDD i el reial decret llei són lleis espanyoles.

5. B · **Minimització de dades**: recollir només el que la finalitat necessita. A més, una al·lèrgia és una dada de salut, una categoria especial.

6. B · Les galetes d'analítica no són estrictament necessàries, així que el consentiment hauria d'arribar **primer**. És una troballa per comunicar amb educació i amb evidències, no la prova d'un atac.

7. A, C · Les lleis **se sumen**: les dades personals hi porten el **RGPD** i la **LOPDGDD**, i el sector i la mida hi porten la **NIS2**. El RGPD s'aplica avui, independentment de la transposició de la NIS2.