
RA7. Legislació i normativa sobre seguretat i protecció de dades

Índex

1. Per què un tècnic de sistemes ha de conèixer la llei	1
2. El marc normatiu de la protecció de dades a Europa i a Espanya	2
2.1 El RGPD (Reglament General de Protecció de Dades)	2
2.2 La LOPDGDD (normativa espanyola)	2
2.3 L'Agència Espanyola de Protecció de Dades (AEPD)	3
2.4 Règim sancionador	3
3. Per què cal controlar l'accés a la informació personal	3
4. Les figures legals en el tractament de dades	4
5. Els drets de les persones sobre les seves dades	4
6. La legislació sobre serveis de la societat de la informació i comerç electrònic	5
6.1 Obligacions d'informació dels llocs web	6
6.2 Comunicacions comercials i correu electrònic (<i>spam</i>)	6
6.3 Cookies	6
7. Normes de gestió de la seguretat de la informació	7
7.1 La família ISO/IEC 27000	7
7.2 L'Esquema Nacional de Seguretat (ENS)	7
7.3 Altres marcs rellevants	7
8. Per què cal respectar la normativa	8

Cicle formatiu: CFGS Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0378. Seguretat i alta disponibilitat

NOTA

Aquest RA és l'únic del mòdul de caràcter íntegrament normatiu: no hi ha una part “de laboratori”, però és tan important com els altres, perquè un administrador de sistemes que desconeixi la legislació pot exposar l'empresa (i ell mateix) a sancions molt greus, encara que la part tècnica estigui ben feta.

1. Per què un tècnic de sistemes ha de conèixer la llei

Quan configurem un servidor Samba AD-DC, un NAS amb dades de clients o una còpia de seguretat amb BackupPC, no només estem prenent decisions tècniques: estem prenent decisions amb conseqüències **legals**. Un fitxer amb noms, DNI i historials mèdics guardat sense xifrar en un recurs compartit accessible per tota l'empresa no és només una mala pràctica de seguretat: pot ser una **infracció greu** sancionable amb milions d'euros.

Com a futur tècnic o tècnica d'ASIX, la teva responsabilitat típica no és redactar les clàusules legals (això és feina del Delegat de Protecció de Dades i dels juristes), però sí:

- Conèixer **quines obligacions tècniques** es deriven de la llei (control d'accés, xifratge, registres, còpies de seguretat, etc.).
- Saber **a qui has d'avisar** si detectes una bretxa de seguretat.
- Entendre per què certes decisions “de negoci” (com enviar comunicacions comercials) tenen implicacions tècniques que tu has d'implementar (l·listes d'exclusió, doble opt-in, etc.).

2. El marc normatiu de la protecció de dades a Europa i a Espanya

2.1 El RGPD (Reglament General de Protecció de Dades)

El **Reglament (UE) 2016/679**, conegut com a **RGPD** (o *GDPR* en anglès), és la norma europea que regula el tractament de dades personals. És directament aplicable a tots els estats membres des del **25 de maig de 2018**, sense necessitat de transposició.

Principis clau del RGPD que afecten directament el disseny de sistemes:

Principi	Què implica tècnicament
Licitud, lleialtat i transparència	Cal saber i documentar per què es guarden les dades
Limitació de la finalitat	No reutilitzar dades recollides per a un fi diferent
Minimització de dades	No emmagatzemar més camps dels necessaris
Exactitud	Mecanismes perquè l'usuari pugui corregir les seves dades
Limitació del termini de conservació	Polítiques de purga/esborrat automàtic
Integritat i confidencialitat	Xifratge, control d'accés, còpies de seguretat
Responsabilitat proactiva (<i>accountability</i>)	Poder demostrar el compliment (registres, auditories)

Un concepte central del RGPD que afecta directament el treball d'un administrador de sistemes és el de **“Privacitat des del disseny i per defecte”** (*Privacy by Design and by Default*, article 25): la seguretat i la privacitat no s'afegeixen al final, s'han de tenir en compte des que es dissenya la infraestructura (per exemple, activar el xifratge de disc per defecte, no deixar oberts ports innecessaris, aplicar el principi de mínim privilegi als comptes AD, etc.).

2.2 La LOPDGDD (normativa espanyola)

A Espanya, la **Llei orgànica 3/2018, de 5 de desembre**, de Protecció de Dades Personals i garantia dels drets digitals (**LOPDGDD**) desenvolupa i completa el RGPD en els aspectes que el mateix reglament deixa marge als estats membres, i deroga l'antiga LOPD 15/1999.

Aspectes rellevants que aporta la LOPDGDD:

- Fixa l'**edat de consentiment digital dels menors en 14 anys** (el RGPD permet als estats triar entre 13 i 16).
- Regula un **títol específic de “drets digitals”** (dret a l'oblit en xarxes, dret a la desconnexió digital, testament digital, educació digital, etc.), únic a la UE.
- Concreta el règim sancionador i els terminis de prescripció de les infraccions.
- Regula els sistemes d'informació de creditícia (fitxers de morosos, tipus ASNEF).
- Regula els sistemes d'informació interna (canals de denúncies) a les organitzacions.

2.3 L'Agència Espanyola de Protecció de Dades (AEPD)

L'**AEPD** és l'autoritat de control independent que vetlla pel compliment de la normativa a Espanya. Entre les seves funcions hi ha:

- Rebre i investigar reclamacions de ciutadans.
- Imposar sancions administratives.
- Publicar guies tècniques (per exemple, sobre xifratge, videovigilància, apps mòbils, cookies) molt útils per a un tècnic de sistemes.
- Gestionar el registre d'activitats de tractament en determinats supòsits.

2.4 Règim sancionador

El RGPD estableix dos nivells de sanció econòmica, que la LOPDGDD adapta:

- **Infraccions lleus/menys greus:** fins a 10 milions d'euros o el 2 % de la facturació anual global (el que sigui més alt).
- **Infraccions greus:** fins a 20 milions d'euros o el 4 % de la facturació anual global.

A més de la multa, l'AEPD pot ordenar mesures correctores (aturar un tractament, notificar als afectats, etc.), que sovint recauen directament sobre l'equip tècnic per executar-les.

3. Per què cal controlar l'accés a la informació personal

El principi de **confidencialitat** del RGPD (article 5.1.f) exigeix que les dades personals es tractin de manera que es garanteixi una seguretat adequada, incloent-hi la protecció contra el tractament no autoritzat o il·lícit.

Des del punt de vista d'un administrador de sistemes, això es tradueix en mesures molt concretes que ja coneixes d'altres RA del mòdul:

- **Control d'accés basat en rols (RBAC):** als grups d'Active Directory, als permisos NTFS/POSIX dels recursos compartits, a les taules d'una base de dades.
- **Principi de mínim privilegi:** un usuari del departament de màrqueting no ha de tenir accés a la nòmina, encara que estiguin al mateix servidor de fitxers.
- **Traçabilitat / auditoria (logging):** registrar qui ha accedit a quines dades i quan (imprescindible per demostrar *accountability* davant l'AEPD).
- **Xifratge en repòs i en trànsit:** discs xifrats (LUKS, BitLocker), connexions xifrades (TLS, VPN/WireGuard), especialment rellevant per a categories especials de dades (salut, ideologia, orientació sexual...), que l'article 9 del RGPD considera **dades especialment protegides**.
- **Segmentació de xarxa:** aïllar els servidors amb dades confidencials (per exemple, un servidor de RRHH) en una VLAN pròpia darrere d'un tallafoc.
- **Política de contrasenyes i autenticació forta (MFA):** reduir el risc d'accés no autoritzat per credencials compromeses.

Un incident típic que il·lustra la importància d'aquest control és la **bretxa de seguretat (data breach)**. Segons l'article 33 del RGPD, si es produeix una violació de seguretat de les dades, el responsable del tractament ha de **notificar-ho a l'AEPD en un termini màxim de 72 hores** des que en té coneixement, i en determinats casos també ha d'informar els afectats

(article 34). Aquí el paper del tècnic de sistemes és clau: sovint és qui detecta l'incident, en fa la contenció tècnica (aïllar el sistema afectat, revocar credencials, etc.) i aporta les evidències (logs) necessàries per a la notificació.

4. Les figures legals en el tractament de dades

El RGPD defineix un conjunt de figures amb responsabilitats diferenciades. Conèixer-les és imprescindible per saber “qui respon de què” dins d'una organització:

Figura	Definició	Exemple
Interessat (<i>data subject</i>)	La persona física a qui pertanyen les dades	Un client, un empleat, un alumne
Responsable del tractament	Qui decideix les finalitats i mitjans del tractament	L'empresa/institut titular de la base de dades
Encarregat del tractament	Qui tracta dades per compte del responsable, en virtut d'un contracte	Una empresa de manteniment informàtic que gestiona els servidors, un proveïdor de <i>hosting</i> o de <i>backup</i> al núvol
Delegat de Protecció de Dades (DPD/DPO)	Figura de supervisió i assessorament interna/externa, obligatòria en molts casos (administracions públiques, tractaments a gran escala, dades confidencials)	El DPO d'un centre educatiu o d'un hospital
Autoritat de control	Organisme independent que supervisa el compliment	L'AEPD (o l'Autoritat Catalana de Protecció de Dades, APDCAT, per a l'àmbit públic català)
Destinatari	Persona o entitat a qui es comuniquen les dades	La Seguretat Social, a qui l'empresa comunica dades laborals

Punt clau per a un tècnic: quan una empresa contracta un servei de còpies de seguretat al núvol, un CRM en SaaS o un servei de correu extern, aquell proveïdor esdevé **encarregat del tractament** i ha d'existir un **contracte d'encarregat de tractament** (article 28 RGPD) que reguli les seves obligacions de seguretat. Si com a tècnic proposes migrar les dades de l'empresa a un servei al núvol, cal assegurar-se que existeix aquest contracte i que el proveïdor ofereix garanties suficients (per exemple, certificacions ISO 27001, ubicació dels servidors dins de l'EEE, etc.).

5. Els drets de les persones sobre les seves dades

El RGPD reconeix un conjunt de drets a l'interessat, coneguts tradicionalment com a **drets ARCO** (Accés, Rectificació, Cancel·lació/Supressió, Oposició), ampliat pel RGPD amb la **portabilitat** i la **limitació del tractament**:

- **Dret d'accés** (art. 15): saber quines dades es tracten i amb quina finalitat.
- **Dret de rectificació** (art. 16): corregir dades inexactes.
- **Dret de supressió / “dret a l'oblit”** (art. 17): sol·licitar l'eliminació de les dades quan ja no siguin necessàries.

- **Dret a la limitació del tractament** (art. 18): “congelar” temporalment l'ús de les dades sense eliminar-les.
- **Dret a la portabilitat** (art. 20): rebre les dades en un format estructurat i d'ús comú per traspassar-les a un altre proveïdor.
- **Dret d'oposició** (art. 21): oposar-se a un tractament concret (per exemple, a rebre publicitat).

Implicacions tècniques d'aquests drets:

Aquests drets no són només un tràmit administratiu: han de poder-se **executar tècnicament** en un termini d'un mes (art. 12.3 RGPD). Això obliga a dissenyar sistemes que permetin:

- Localitzar totes les dades d'una persona en totes les bases de dades i sistemes de fitxers (fins i tot en còpies de seguretat).
- Exportar-les en un format estàndard (per exemple, JSON o CSV) per atendre una sol·licitud de portabilitat.
- Esborrar-les de forma efectiva (i no només “marcar-les com a esborrades”), tenint en compte que les còpies de seguretat també contenen dades personals i s'han de gestionar amb una política de retenció coherent.
- Documentar l'atenció de la sol·licitud (qui l'ha atesa, quan, què s'ha fet) per poder demostrar-ho.

NOTA

Un error freqüent és pensar que “esborrar un registre de la base de dades” ja compleix el dret de supressió. Si aquell registre segueix present en 30 còpies de seguretat diàries que es conserven durant un any, la dada continua existint. Cal una política de retenció i rotació de còpies coherent amb els terminis de conservació establerts.

6. La legislació sobre serveis de la societat de la informació i comerç electrònic

A banda de la protecció de dades, l'administrador de sistemes s'enfronta sovint a un altre bloc normatiu: la **Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI-CE)**.

Aquesta llei regula, entre d'altres:

6.1 Obligacions d'informació dels llocs web

Tot lloc web que ofereixi béns o serveis (o simplement representi una activitat econòmica) ha de mostrar de forma fàcilment accessible:

- Nom o denominació social del titular.
- NIF/CIF.
- Domicili.
- Adreça de correu electrònic de contacte.
- Dades registrals, si escau (registre mercantil, col·legi professional, etc.).

Aquesta informació sol aparèixer en un “**Avís legal**”, que com a tècnic potser hauràs d'ajudar a implementar dins del gestor de continguts (WordPress, per exemple).

6.2 Comunicacions comercials i correu electrònic (*spam*)

Aquest és el punt de contacte més directe amb la infraestructura tècnica que administrareu (servidors de correu com Postfix, Kea DHCP + BIND9, o serveis SaaS de màrqueting):

- Es prohibeix l'enviament de comunicacions comercials per correu electrònic **sense el consentiment previ i exprés del destinatari** (règim d'*opt-in*, article 21 LSSI-CE).
- Cal oferir sempre un mecanisme senzill i gratuït per **donar-se de baixa** (*opt-out*) de futures comunicacions.
- L'incompliment d'aquestes obligacions es considera **spam** i és sancionable.

Implicacions tècniques:

- Configuració de llistes de distribució amb **dobles opt-in** (l'usuari confirma la subscripció des del seu propi correu).
- Manteniment d'una **llista de supressió/exclusió** (*suppression list*) que impedeixi tornar a enviar correus a qui s'hi ha donat de baixa, encara que torni a aparèixer en una importació de dades.
- Registres (*logs*) que demostrin quan i com es va obtenir el consentiment.

6.3 Cookies

Encara dins l'àmbit de la LSSI-CE (article 22.2, modificat per adaptar la Directiva ePrivacy), la instal·lació de cookies no tècnicament necessàries (analítiques, publicitàries, de xarxes socials) **requereix el consentiment informat i explícit** de l'usuari abans d'instal·lar-les, mitjançant un banner de cookies que permeti acceptar, rebutjar i configurar amb la mateixa facilitat.

7. Normes de gestió de la seguretat de la informació

Més enllà de les lleis (d'obligat compliment), existeixen **normes tècniques i estàndards de gestió**, majoritàriament voluntaris, que ajuden les organitzacions a estructurar la seva seguretat i, en molts casos, a poder demostrar el compliment legal (*accountability*).

7.1 La família ISO/IEC 27000

- **ISO/IEC 27001**: especifica els requisits per implantar un **Sistema de Gestió de la Seguretat de la Informació (SGSI)**. És l'única norma certificable de la família: una empresa es pot auditar i obtenir el certificat ISO 27001.
- **ISO/IEC 27002**: catàleg de bones pràctiques i controls de seguretat (organitzatius, tècnics, físics) que complementa la 27001.
- **ISO/IEC 27005**: metodologia de gestió del risc en seguretat de la informació.
- **ISO/IEC 27701**: extensió per a la gestió de la privacitat (PIMS), molt lligada al RGPD.

El cicle de millora contínua PDCA (*Plan-Do-Check-Act*) és el nucli metodològic de la 27001: planificar els controls, implantar-los, revisar-ne l'eficàcia i actuar sobre les desviacions.

7.2 L'Esquema Nacional de Seguretat (ENS)

A Espanya, les administracions públiques (i moltes empreses que hi prestin serveis) estan obligades a complir l'**Esquema Nacional de Seguretat (ENS)**, regulat pel Reial decret 311/2022. L'ENS estableix:

- Categorització dels sistemes en nivells (BÀSIC, MITJÀ, ALT) segons l'impacte que tindria un incident.
- Un conjunt de mesures de seguretat obligatòries per categoria (marc organitzatiu, operacional i de protecció).
- L'obligació d'auditar periòdicament el compliment.

Per a un institut públic com el vostre centre, l'ENS és directament aplicable als sistemes que tracten dades de l'alumnat.

7.3 Altres marcs rellevants

- **NIST Cybersecurity Framework**: marc de referència (nord-americà, però àmpliament adoptat) organitzat en cinc funcions: Identificar, Protegir, Detectar, Respondre i Recuperar.
- **Directiva NIS2** (transposada progressivament als estats membres de la UE): amplia les obligacions de ciberseguretat a operadors de serveis essencials i importants (energia, salut, administració, alguns proveïdors digitals), amb requisits de gestió de risc, notificació d'incidents i responsabilitat de la direcció.

NOTA

Diferència clau La llei (RGPD, LOPDGDD, LSSI-CE) és **d'obligat compliment** i preveu sancions. Les **normes tècniques** (ISO 27001, ENS quan no és administració pública,

NIST) solen ser **voluntàries**, però ajuden a complir la llei de manera demostrable i són sovint exigides contractualment per clients o socis.

8. Per què cal respectar la normativa

Més enllà de la por a la sanció econòmica, hi ha raons de fons per interioritzar aquesta normativa com a part de la professionalitat tècnica:

1. **Protecció de drets fonamentals:** la protecció de dades no és un tràmit burocràtic, és un dret fonamental (article 18.4 de la Constitució espanyola i article 8 de la Carta de Drets Fonamentals de la UE). Darrere de cada base de dades hi ha persones reals que poden patir perjudicis (discriminació, frau, dany reputacional) si les seves dades es filtren o s'usen malament.
2. **Confiança i reputació:** una bretxa de seguretat mal gestionada té un cost reputacional que sovint supera la mateixa sanció econòmica.
3. **Responsabilitat professional i personal:** en determinats casos, l'incompliment greu i intencionat pot comportar també responsabilitat penal (per exemple, delictes de descobriment i revelació de secrets, articles 197 i següents del Codi penal).
4. **Ètica professional:** com a tècnics, sovint som els únics que realment “veiem” les dades en brut (logs, bases de dades, còpies de seguretat). Aquest accés privilegiat comporta una responsabilitat ètica afegida.
5. **Competitivitat:** cada cop més clients i administracions exigeixen contractualment el compliment normatiu (RGPD, ENS, ISO 27001) com a requisit per contractar un servei, de manera que complir la llei també és una qüestió de negoci.

Versions d'aquest document

- [HTML](#)
- [PDF](#)
- [ODT](#)
- [MD](#)

[Domini Públic \(CC0\)](#)