Mòdul 0226 — Seguretat Informàtica

Índex

Cicle formatiu: Sistemes Microinformàtics i Xarxes (SMX)

Durada total: 132 hores (99 al centre + 33 a l'empresa)

RA1 --- Seguretat Passiva

1.1. Conceptes bàsics de seguretat informàtica

La **seguretat informàtica** és la disciplina que dissenya normes, procediments, mètodes i tècniques per aconseguir que un Sistema d'Informació (SI) sigui segur i confiable.

Elements a protegir d'un SI

Element	Descripció	Exemples
Maquinari	Components físics	Ordinadors, perifèrics, cables, discos
Programari	Elements lògics	Sistema operatiu, aplicacions, webs
Informació	Les dades processades	Fitxers, bases de dades, documents
Usuaris	Persones que interactuen amb el sistema	Empleats, administradors, clients

Propietats d'un SI segur (CIA + No repudi)

- **Integritat**: la informació ha de ser exacta i completa.
- **Confidencialitat**: només les persones autoritzades poden accedir-hi o modificar-la.
- **Disponibilitat**: la informació ha d'estar disponible quan els usuaris la necessiten.
- **No repudi** *(desitjable)*: s'ha de poder provar la participació de les parts en una comunicació.

Classificació dels mecanismes de seguretat

Segons el que protegeixen:

- **Seguretat Física**: protegeix el maquinari (actiu físic).
- **Seguretat Lògica**: protegeix dades, aplicacions i sistemes operatius (actiu lògic).

Segons quan actuen:

- **Seguretat Activa**: actua *abans* del problema per evitar danys (contrasenyes, antivirus, tallafocs).
- **Seguretat Passiva**: actua *després* del problema per minimitzar efectes i facilitar la recuperació (còpies de seguretat, SAI, logs).

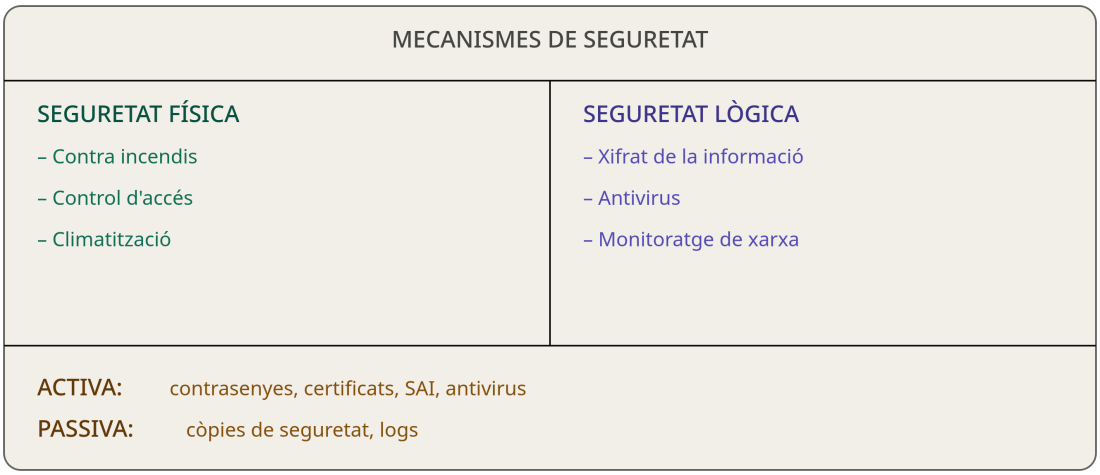

Figura 1: Classificació dels mecanismes de seguretat

Recorda: La seguretat activa prevé; la seguretat passiva recupera.

1.2. Seguretat física: el CPD i les instal·lacions

La **seguretat física** protegeix el maquinari de les amenaces com desastres naturals, incendis, sobrecàrregues elèctriques, robatoris i accessos no autoritzats.

El Centre de Processament de Dades (CPD / Data Center)

Un CPD centralitza les operacions i infraestructura d'una organització: s'hi emmagatzemen, processen i gestionen les dades i aplicacions del SI.

Avantatges d'un CPD:

- Augment de la seguretat
- Eficiència energètica
- Reducció de costos
- Escalabilitat

Ubicació de les instal·lacions

A l'hora de triar on ubicar un CPD cal tenir en compte:

- **Desastres naturals**: evitar zones inundables, sísmiques i inestables.
- **Connectivitat i energia**: accés a fibra òptica de qualitat i possibilitat de dos proveïdors elèctrics.
- **Factors externs**: proximitat a bombers i policia, taxes de criminalitat baixes.

Control ambiental

Factor	Valor recomanat	Risc si no es compleix
Temperatura	24 °C estable	Sobreescalfament dels equips
Humitat relativa	50%	Alta → corrosió / Baixa → curtcircuits
Pols	Neteja periòdica	Acumulació i fallada de components
EM	Apantallament de cables / fibra òptica	Interferències que corromprien dades

La ventilació als CPD s'organitza en *passadissos freds i calents* per gestionar eficientment la temperatura als racks.

Instal·lacions elèctriques

- **SAI (Sistema d'Alimentació Ininterrompuda / UPS)**: bateries que proporcionen energia temporal en cas de tall elèctric. Vegeu secció 1.3.
- **Grup electrogen**: generador amb motor de combustió (dièsel). S'ubica als terrats. Per a sistemes crítics com hospitals o emergències.

Sistemes d'extinció d'incendis

- **Materials ignífugs**: eviten la propagació del foc als racks i parets.
- **Detectors d'incendis**: sistemes òptics que detecten fum i partícules de combustió.
- **Sistemes d'extinció**:
  - *Extintors CO_2*: redueixen l'oxigen al focus de l'incendi.
  - *Gasos fluorats*: absorbeixen calor per apagar les flames.
  - *Reducció d'oxigen*: extreu l'oxigen de l'ambient.

  Nota: Mai s'utilitza aigua en CPD per risc de curtcircuit.

Control d'accessos

- **Mesures dissuasives**: tanques, guàrdies de seguretat, alarmes, portes blindades.
- **Control físic d'accés**: panys, targetes magnètiques, RFID, teclat numèric, sistemes biomètrics.
- **Detecció d'intrusos**: càmeres de seguretat, sensors de moviment i temperatura, alarmes als punts d'accés.

1.3. Sistemes d'Alimentació Ininterrompuda (SAI)

Un **SAI** és un conjunt de bateries que alimenta una instal·lació elèctrica. En cas de tall, els equips connectats continuen funcionant gràcies a les bateries.

Preguntes clau per triar un SAI

1. Quants **watts** consumeixen els equips a protegir?
2. Quant de **temps** necessito mantenir-los operatius?

Problemes que soluciona un SAI

- Talls d'energia
- Microtalls i baixades de voltatge momentànies
- Pics de tensió (alt voltatge momentani)
- Pujades/baixades de tensió sostingudes
- Acció dels llamps
- Soroll elèctric i distorsió harmònica

Tipus de SAI

Tipus	Protecció	Temps de transferència	Ús típic
Off-line / Stand-By	Bàsica (talls i variacions)	2--10 ms	PC domèstics, monitors, TV
In-line / Interactiva	Intermèdia (+ sorolls, analitza qualitat)	2--10 ms	Routers, commutadors, càmeres
On-line	Alta (sempre actiu, sense temps de transferència)	0 ms	CPD, telecomunicacions, indústria

> Els SAI *on-line* requereixen substitució de bateries més sovint, però ofereixen la millor protecció.

Fórmules bàsiques

```
Watts = Volts × Amperis
VA = Watts / 0,7          (factor de conversió)
Marge de seguretat = +25% (per a futures ampliacions)

Minuts extra del SAI = Temps del SAI × (VA_SAI / VA_dispositius) ×
 ↪  Factor de temps
  Factor de temps: fins a 3 min → 1,3 | més de 3 min → 1,5
```

NOTA

El factor 0,7 és una aproximació orientativa per a equips de consum. En entorns de CPD el factor de potència real sol ser 0,9–0,99; consulta sempre les especificacions dels equips.

Exemple: Equips que consumeixen 230 V × 1,5 A = 345 W → VA = 345 / 0,7 ≈ 493 VA. Amb marge del 25% → SAI mínim de **616 VA**.

Manteniment del SAI

- Revisar regularment l'estat de les bateries.
- La substitució l'ha de fer personal qualificat (risc per a l'electròlit).
- No llençar al foc (explosió) ni abandonar a la natura (contaminació).
- Les marques habituals inclouen: APC, Salicru, Riello, Belkin, Zigor.

  Alternativa econòmica: Les *regletes protectores* protegeixen de pujades de tensió i soroll elèctric, però **no** protegeixen dels talls d'energia.

1.4. Seguretat lògica: control d'accés i contrasenyes

La **seguretat lògica** controla l'accés als equips informàtics verificant la identitat de les persones.

Conceptes clau

- **Objecte**: recurs amb accés controlat (fitxers, directoris, pàgines de memòria, programes).
- **Subjecte**: usuari o entitat que accedeix als objectes mitjançant un procés.
- **Dret d'accés**: com un subjecte pot accedir a un objecte (lectura, escriptura, execució).

Funcions del control d'accés

Autenticació: verificar la identitat de l'usuari.

- Per **coneixement**: alguna cosa que sap (contrasenya, PIN).
- Per **possessió**: alguna cosa que té (targeta, token).
- Per **característica**: alguna cosa que és (biometria).

Autorització: concedir permisos per accedir a un recurs concret.

Política de contrasenyes

Una política de contrasenyes regula les normes de creació, protecció i renovació.

Requisits d'una contrasenya robusta:

- Barreja de majúscules i minúscules.
- Combinació de lletres, números i caràcters especials.
- Mínim **10 caràcters** de longitud.
- No ha d'aparèixer en cap diccionari.
- No s'ha de basar en informació personal (nom, data de naixement…).

Normes de protecció:

- Mai escriure la contrasenya en un correu electrònic.
- No dir-la per telèfon ni a companys, ni que siguin superiors.
- No escriure-la en papers ni formularis.
- No posar pistes de la contrasenya.
- Canviar-la cada **sis mesos** com a mínim.

Sistemes biomètrics

Els **sistemes biomètrics** verifiquen la identitat analitzant atributs físics o comportamentals de l'usuari.

Tipus més comuns:

- Lectors d'empremtes dactilars
- Lectors del palmell de la mà
- Lectors de retina
- Lectors d'iris
- Reconeixement facial

Errors possibles:

- **Fals positiu (FP)**: el sistema accepta un impostor que hauria de ser denegat. *(Error greu)*
- **Fals negatiu (FN)**: el sistema denega l'accés a un usuari legítim.

  Els sistemes biomètrics són molt més robustos que les contrasenyes, però també més costosos i poden generar problemes de privadesa.

RA2 --- Gestió de Dispositius d'Emmagatzematge

2.1. Tipus d'emmagatzematge

Classificació de la memòria

- **Volàtil / No volàtil**: perd o conserva les dades sense alimentació.
- **Lectura / Lectura-Escriptura**: ROM vs. RAM.
- **Primària / Secundària**: memòria principal vs. emmagatzematge persistent.
- **Accés seqüencial / Aleatori**: cintes magnètiques vs. discos/SSD.

Principals sistemes d'emmagatzematge

Sistema	Característiques
Local	Discos durs, SSD, mòbils, tauletes
Servidors en xarxa	Informació centralitzada al servidor
Dispositius externs	Cintes, HDD extern, CD/DVD, USB
Còpies de seguretat	Automàtiques o manuals
Núvol (Cloud)	Dropbox, Google Drive, OneDrive, NextCloud…

Arquitectures d'emmagatzematge en xarxa

DAS (Direct Attached Storage)

- Connexió directa al servidor (SATA, SAS, USB, SCSI).
- Solució econòmica i fàcil de gestionar.
- *Problema*: si el servidor cau, no es pot accedir a les dades compartides.

NAS (Network Attached Storage)

- Comparteix, centralitza i connecta tota la xarxa local.
- Usa protocols SMB/CIFS i requereix un sistema operatiu propi.
- Avantatges: accés remot, streaming, còpies automàtiques.
- *Problema*: rendiment limitat per l'ús compartit de la xarxa.

SAN (Storage Area Network)

- Xarxa paral·lela a la LAN dedicada a dades crítiques.
- Usa fibra òptica i protocols FCP, iSCSI, FCoE.
- Tres capes: host → fibra → emmagatzematge.
- Accés ràpid i confiable entre servidors i recursos d'emmagatzematge.

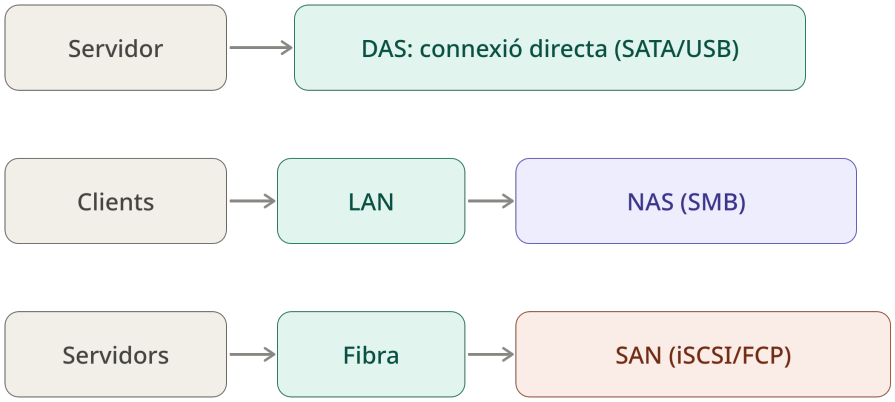

Figura 2: Arquitectures d'emmagatzematge

Destrucció segura de dades

Quan cal eliminar dades de forma permanent:

1. **Programari d'esborrament**: substitueix cada bit per zeros o dades aleatòries (Algoritme Gutmann: 35 passades).
2. **Desmagnetització**: camp magnètic potent que desimanta els dominis magnètics.
3. **Destrucció física**: triturar el disc en fragments molt petits.

2.2. RAID: emmagatzematge redundant

RAID (*Redundant Array of Independent Disks*) utilitza diversos discos físics configurats com una única unitat lògica per aconseguir major capacitat, seguretat i menor cost.

Implementació

- **Maquinari**: controladora a la placa base o targeta d'expansió.
- **Programari**: el sistema operatiu gestiona els discos amb la controladora convencional.

Tipus de RAID

RAID 0 --- Striping (distribució)

- La informació es reparteix entre *tots* els discos disponibles.
- Permet lectura i escriptura simultànies → màxima velocitat.
- **Cap redundància**: si un disc falla, es perd tota la informació.
- *Ús*: usuaris domèstics sense dades crítiques.

```
Disc 1: [A1][A3][A5]
Disc 2: [A2][A4][A6]   ← Les dades es reparteixen en tires (stripes)
```

RAID 1 --- Mirror (mirall)

- Duplica la informació a cada disc simultàniament.
- Si un disc falla, l'altre conté tota la informació.
- Cost baix, però perd el 50% de la capacitat total.
- *Ús*: servidors que necessiten disponibilitat contínua.

```
Disc 1: [A][B][C]
Disc 2: [A][B][C]   ← Còpia exacta
```

RAID 5 --- Striping amb paritat

- Mínim **3 discos**. Distribueix dades i paritat entre tots.
- Si falla *un* disc, es reconstrueix la informació amb la paritat.
- Bon equilibri entre rendiment, capacitat i redundància.
- *Ús*: dades crítiques (hospitals, empreses).

RAID 6 --- Striping amb doble paritat

- Mínim **4 discos**. Pot suportar la fallada de *dos* discos simultanis.
- Alta fiabilitat per a entorns CPD.

RAID 10 (0+1) --- Striping + Mirror

- Combina la velocitat del RAID 0 amb la redundància del RAID 1.
- Millora la seguretat i el rendiment alhora.
- Requereix com a mínim **4 discos**.

RAID	Discos mínims	Redundància	Velocitat	Capacitat útil	Ús típic
0	2	Cap	Molt alta	100%	Usuari domèstic
1	2	Total	Alta	50%	Servidors
5	3	Un disc	Alta	(n-1)/n	Empreses
6	4	Dos discos	Mitja	(n-2)/n	CPD
10	4	Total (mirall)	Molt alta	50%	CPD crític

2.3. Còpies de seguretat

Per què fer còpies?

- Protegir davant fallades del sistema o desastres naturals.
- Protegir davant esborrades accidentals d'usuaris.
- Protegir davant atacs (especialment ransomware).

  L'Agència Espanyola de Protecció de Dades (AEPD) **obliga** les empreses a realitzar còpies de seguretat de les dades personals.

Classificació de la informació

- **Confidencial**: dada conficencial d'accés restringit.
- **Interna**: accessible a tots els usuaris de l'organització.
- **Pública**: sense cap restricció d'accés.

Mètodes de còpia per granularitat

Mètode	Descripció	Restauració	Espai usat
Còpia completa (Total)	Còpia de totes les dades seleccionades	Ràpida (un sol suport)	Màxim
Còpia diferencial	Dades modificades des de l'última còpia **completa**	Mitja (completa + diferencial)	Intermedi
Còpia incremental	Dades modificades des de l'última còpia (de qualsevol mena)	Lenta (completa + totes les incrementals)	Mínim

```
EXEMPLE D'ESTRATÈGIA SETMANAL:

Dilluns:   Còpia COMPLETA     (T)
Dimarts:   Còpia INCREMENTAL  (I1) ← canvis des de T
Dimecres:  Còpia INCREMENTAL  (I2) ← canvis des de I1
Dijous:    Còpia INCREMENTAL  (I3) ← canvis des de I2

Restauració divendres: T + I1 + I2 + I3
```

Estratègies recomanades

- **Total diària**: màxima seguretat, màxim espai.
- **Total setmanal + Diferencial diària**: bon equilibri.
- **Total setmanal + Incremental diària**: mínim espai, restauració més lenta.

Paràmetres de temps

- **RPO (Recovery Point Objective)**: període màxim de dades que es pot perdre.
- **RTO (Recovery Time Objective)**: temps màxim que el sistema pot estar aturat.

Ubicació de les còpies

- **En línia interna**: mateixa màquina o RAID. Risc: es pot perdre tot alhora.
- **En línia externa**: cloud, servidor Linux (cron + rsync). Recomanat.
- **Exterior**: caixa forta, altre edifici. Màxima seguretat física.

Còpies en calent vs. en fred

- **En fred**: el sistema no és accessible durant la còpia. Dades estables.
- **En calent**: el sistema segueix operatiu durant la còpia. Necessita major precisió.

Eines i conceptes addicionals

- **Punt de restauració** (Windows): snapshot de l'estat del sistema. Irreversible un cop llançat.
- **LiveCD de Linux**: arrenca l'ordinador des d'un CD/USB per clonar discos independentment del SO.
- **Congelació**: programari que recorda l'estat del sistema (*snapshot*) i descarta tots els canvis en reiniciar. Exemple típic: cibercafè.

2.4. Criptografia

Concepte

La **criptografia** (*kriptós* = ocult + *graphos* = escriptura) transforma un document original mitjançant un algorisme per obtenir un document il·legible. El destinatari aplica el procés invers amb la clau correcta.

> Objectiu: si algú intercepta el missatge, no en pugui entendre el contingut.

Vegeu GNU Privacy Guard (GPG)

Criptografia simètrica

- **Mateixa clau** per xifrar i desxifrar.
- Senzilla d'usar, ràpida.
- *Problema*: com es transmet la clau de forma segura?
- Algorismes: **DES, 3DES, AES, Blowfish, IDEA**.

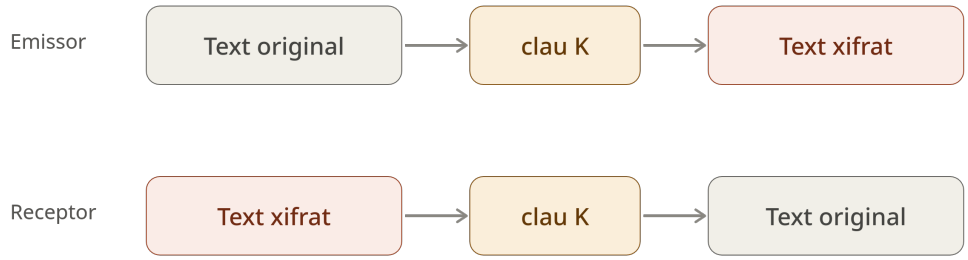

Figura 3: La mateixa clau K xifra i desxifra

Criptografia asimètrica (clau pública/privada)

- Creada per **Diffie i Hellman**.
- Cada persona té un **parell de claus**: pública (distribuïble) i privada (secreta).
- El que es xifra amb la clau pública només es pot desxifrar amb la clau privada, i viceversa.

Procés d'enviament d'un missatge xifrat:

1. El receptor genera el parell de claus i publica la clau pública.
2. L'emissor xifra el missatge amb la clau pública del receptor.
3. El receptor desxifra amb la seva clau privada.

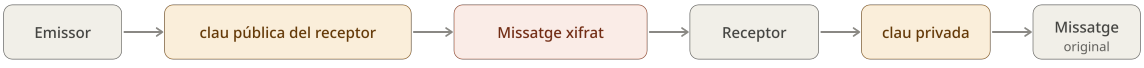

Figura 4: Xifrat amb clau pública del receptor

AVÍS

Els ordinadors quàntics podrien posar en risc els sistemes actuals de criptografia asimètrica pel seu enorme poder de càlcul.

Eines pràctiques

- **GnuPG**: eina per signar, xifrar i desxifrar texts, correus i fitxers.
- **Ubuntu Keyserver**: servidor de claus públiques.
- **Mailvelope**: extensió per xifrar correus de punta a punta en el navegador.
- **GpgFrontend**: interfície gràfica multiplataforma per a GnuPG.

RA3 --- Seguretat Activa

3.1. Programari maliciós (Malware)

El **malware** (*malicious software*) és qualsevol programa dissenyat per infiltrar-se en un dispositiu sense el consentiment de l'usuari, amb l'objectiu de robar, xifrar, esborrar dades o prendre el control del sistema.

Tipus principals de malware

Virus

- Necessita un **fitxer portador** per propagar-se (document, executable).
- S'activa quan l'usuari executa el fitxer infectat.
- Objectiu: replicar-se infectant altres programes.
- *Analogia*: com la grip (necessita un hoste).

Cucs (Worms)

- **Autònoms**: no necessiten fitxer portador.
- S'estenen per la xarxa explotant vulnerabilitats o enginyeria social.
- Objectiu: reproduir-se massivament i col·lapsar xarxes per saturació.
- *Analogia*: un viatger independent que es mou sol.

Troians (Cavalls de Troia)

- Es disfressen de programari legítim (joc, eina, actualització).
- **No es repliquen** sols; l'usuari l'instal·la voluntàriament.
- Objectiu: crear una “porta del darrere” per al control remot, robatori de dades (contrasenyes, dades bancàries) o instal·lació d'altres malware.
- *Analogia*: El Cavall de Troia grec.

Ransomware

- Xifra els fitxers de la víctima amb una clau que només l'atacant coneix.
- Exigeix un **rescat econòmic** (normalment en criptomonedes) per desxifrar-los.
- Arriba com un troià o un cuc (adjunts de correu, webs fraudulentes).
- *La millor defensa*: còpies de seguretat actualitzades.

	Virus	Cuc	Troià	Ransomware
Com es propaga	Fitxer portador + acció usuari	Xarxa, autònom	Engany a l'usuari	Via troià o cuc
Es replica sol	Sí	Sí	No	No
Objectiu principal	Infectar fitxers	Col·lapsar xarxes	Control remot / robatori	Rescat econòmic

Vies d'entrada del malware

- Pàgines web piratejades o amb anuncis maliciosos.
- Fitxers adjunts en correus electrònics (malspam).
- Descàrrega de programari de fonts desconegudes.
- Xarxes P2P.
- Aplicacions mòbils no oficials.

Signes d'alerta en un correu maliciós:

- Remitent sospitós o no esperat.
- Assumpte alarmista o urgent.
- Errors ortogràfics i mala traducció.
- Enllaços que no coincideixen amb el text en passar el ratolí per sobre.
- Adjunts no sol·licitats.

Símptomes d'infecció

1. Lentitud inusual del sistema o la xarxa.
2. Allau d'anuncis emergents (pop-ups).
3. Bloquejos i errors freqüents sense causa aparent.
4. Canvis inesperats (pàgina d'inici del navegador, barres d'eines noves, fitxers desapareguts).
5. L'antivirus es desactiva sol.

Mesures de protecció

- **Mantenir el sistema actualitzat**: els pegats de seguretat corregeixen vulnerabilitats conegudes.
- **Antivirus i antimalware actius i actualitzats**: bloquejar amenaces abans que arribin.
- **Antispam i antispyware** com a capes addicionals.
- **Desconfiar i verificar**: no clicar en enllaços o adjunts sospitosos.
- **Còpies de seguretat regulars**: la millor defensa contra el ransomware.
- **Revisar els permisos de les apps**: no concedir més permisos dels necessaris.

Recursos en cas d'infecció (Espanya)

- **INCIBE** --- Telèfon gratuït: **017**
- Web: https://www.incibe.es/ciudadania/herramientas
- Eines gratuïtes: Conan Mobile (Android), Servei Antibotnet, antivirus, antispyware, analitzadors de fitxers.

Passos en cas d'infecció:

1. Desconnectar de la xarxa.
2. Escanejar i eliminar el programari maliciós amb un programa de seguretat.
3. Canviar totes les contrasenyes (correu, bancs, xarxes socials).
4. Restaurar el sistema des d'una còpia de seguretat neta.
5. Contactar amb l'INCIBE si cal ajuda especialitzada.

3.2. Tallafocs (Firewall) amb iptables

Un **tallafocs** és un dispositiu de seguretat (físic o programari) que filtra el trànsit entre xarxes a partir de regles definides. Pot ser un router, una màquina dedicada o un programa al sistema operatiu.

Funció del tallafocs

Decideix si un paquet de xarxa:

- **Passa** (ACCEPT)
- **Es descarta** (DROP)
- **Es modifica** (NAT, MANGLE)

Tipus d'arquitectures

Tallafocs en encaminador (router)

- Màquines públiques i privades comparteixen la mateixa xarxa.
- Usa llistes de control d'accés (ACL) per filtrar IP i trànsit.

Tallafocs en una màquina (DMZ)

- Separa la xarxa en: xarxa privada interna (LAN) + zona desmilitaritzada (DMZ).
- Els servidors públics (web, mail) van a la DMZ.

Tallafocs de tres direccions

- Una sola màquina amb tres interfícies: WAN + DMZ + LAN.
- Arquitectura molt habitual en empreses mitjanes.

Tallafocs de múltiples màquines

- Diverses màquines protegint la xarxa → major seguretat.

Polítiques del tallafocs

Política	Descripció	Avantatge	Risc
Per defecte ACCEPTAR	Tot passa excepte el que es denega explícitament	Fàcil de gestionar	Ports oberts per desconeixement
Per defecte DENEGAR	Tot bloquejat excepte el que es permet explícitament	Màxima seguretat	Configuració complexa

CONSELL

Recomanació: política per defecte **DENEGAR**. Però cal dominar el sistema per no bloquejar serveis essencials.

AVÍS

Importantíssim: l'**ordre de les regles és determinant**. Es comprova cada regla en ordre i s'aplica la primera que coincideix. Les regles posteriors no s'avaluen per a aquell paquet.

iptables a Linux

`iptables` és l'eina estàndard per gestionar el tallafocs al nucli Linux.

Tres tipus de regles:

- **MANGLE**: modifica capçaleres dels paquets.
- **NAT**: `PREROUTING` i `POSTROUTING` per redireccions i canvis d'IP.
- **FILTER**: `INPUT` (paquets entrants a la màquina), `OUTPUT` (paquets sortints de la màquina), `FORWARD` (paquets que passen per la màquina cap a una altra xarxa).

Comandes bàsiques:

```
# Veure les regles actuals
iptables -L -v -n

# Establir política per defecte DENEGAR (recomanat)
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Permetre trànsit des d'una IP concreta
iptables -A INPUT -s 195.65.34.234 -j ACCEPT

# Permetre accés a MySQL des d'una IP específica
iptables -A INPUT -s 231.45.134.23 -p tcp --dport 3306 -j ACCEPT

# Obrir el port 80 (HTTP) per a tothom
iptables -A INPUT -p tcp --dport 80 -j ACCEPT


# Amb política INPUT DROP, les línies DROP següents són redundants
```

```
# però s'inclouen per claredat pedagògica (mostren que estos ports
 ↪  estan tancats)
# Bloquejar la resta de ports sensibles
iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -A INPUT -p tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp --dport 10000 -j DROP

# Eliminar totes les regles (COMPTE: deixa la màquina oberta)
iptables -F

# Guardar les regles (Debian/Ubuntu)
iptables-save > /etc/iptables/rules.v4
```

Regles NAT (exemple de redireccions):

```
# Activar NAT per a tota la xarxa sortint per eth0
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Redirigir el port 80 extern al port 8080 intern
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port
 ↪  8080
```

3.3. Política de contrasenyes i recuperació de dades

Gestors de contrasenyes

Per als entorns professionals es recomana l'ús de **gestors de contrasenyes** (Bitwarden, KeePass, etc.) en lloc de memòries o papers. Permeten generar i emmagatzemar contrasenyes llargues i aleatòries per a cada servei.

Autenticació multifactor (MFA)

Combina dos o més factors d'autenticació:

- *Alguna cosa que saps* + *alguna cosa que tens* (contrasenya + codi SMS/app)
- Dificulta enormement l'accés als atacants fins i tot si reben la contrasenya.

Recuperació de dades

- Eines com **TestDisk** o **PhotoRec** permeten recuperar particions i fitxers eliminats.
- En casos de disc danyat físicament, cal una empresa especialitzada en sala blanca.
- Un RAID no és una substitució de les còpies de seguretat.

RA4 --- Privadesa a les Xarxes

4.1. Monitoratge de xarxes i sniffers

Gestió de la seguretat a la xarxa

Implica: planificar instal·lacions, documentar, indicar procediments, monitorar i auditar.

El **monitoratge de xarxa** usa programari per conèixer l'estat i fiabilitat de la xarxa: detecta dispositius que fallen, recursos sobrecarregats i analitza el flux de trànsit.

Inventari i control de serveis

Per controlar els serveis d'una xarxa cal:

- **Rangs d'adreces IP privades**:
  - Classe A: `10.0.0.0 -- 10.255.255.255`
  - Classe B: `172.16.0.0 -- 172.31.255.255`
  - Classe C: `192.168.0.0 -- 192.168.255.255`
- **Assignació d'IP**: dinàmica (DHCP) o estàtica.
- **Inventari de MACs**: identificador únic de cada dispositiu.
- **Ports TCP/UDP actius**: cada servei usa un port específic.
  - HTTP: 80 | HTTPS: 443 | SSH: 22 | FTP: 20/21 | MySQL: 3306
- **SNMP**: permet gestió remota i centralitzada dels recursos de xarxa.

Dispositius de control de xarxa

Dispositiu	Funció
Encaminadors/Commutadors	Fan circular la informació per la xarxa
Tallafocs	Permeten o deneguen paquets segons regles
IDS (Intrusion Detection System)	Detecten paquets que indiquen possible atac
Sistemes de monitoratge	Avaluen rendiment, envien alertes (ex: ping als servidors)

Sniffers (detectores de paquets)

Un **sniffer** és qualsevol programa que monitora i analitza els paquets que circulen per una xarxa.

- *Ús legítim*: diagnòstic de xarxa per part d'administradors.
- *Ús maliciós*: un atacant pot capturar contrasenyes, números de targeta i informació confidencial.

Com protegir-se dels sniffers:

- **Xifrat de fitxers i correus**: PGP/GnuPG.
- **SSL/TLS**: canal xifrat entre dos punts (HTTPS entre usuari i servidor).
- **VPN**: xarxa virtual xifrada sobre una xarxa pública.

4.2. Seguretat en xarxes sense fils

Les xarxes WiFi transmeten dades per radiofreqüència (ones electromagnètiques), la qual cosa les fa intrínsecament més exposades que les xarxes cablejades.

Protocols de seguretat WiFi

Protocol	Seguretat	Característiques
WEP	Insegur	Primer protocol WiFi. La clau es pot esbrinar fàcilment.
WPA	Segur	Soluciona autenticació i confidencialitat. Modes: WPA-PSK i 802.1X.
WPA2	Segur	Afegeix xifratge AES. Àmpliament desplegat, però WPA3 ja és el nou estàndard.
WPA3	Molt segur	Estàndard actual des de 2020. Recomanat en tots els nous desplegaments.

CONSELL

Mai usar WEP. Usar WPA2 com a mínim, preferentment WPA3.

Mesures de seguretat WiFi recomanades

- Canviar la contrasenya per defecte del router.
- Usar xifrat WPA2/WPA3.
- Ocultar el SSID (nom de la xarxa) quan sigui possible.
- Filtrar per adreça MAC.
- Monitorar els dispositius connectats regularment.
- Crear una xarxa d'invitats separada de la xarxa corporativa.

4.3. Signatura electrònica i certificats digitals

Signatura electrònica

La **signatura electrònica** garanteix:

- **Autenticitat**: el document prové de qui diu ser.
- **Integritat**: el document no ha estat modificat.
- **No repudi**: el signant no pot negar haver signat.

Funciona amb criptografia asimètrica: el signant xifra un resum (*hash*) del document amb la seva **clau privada**. El receptor el verifica amb la **clau pública** del signant.

Certificat digital

Un **certificat digital** és un document electrònic que:

- Associa una clau pública amb la identitat d'una persona o entitat.
- Està emès i firmat per una **Autoritat de Certificació (CA)** de confiança.
- Exemples de CA a Espanya: FNMT (Fàbrica Nacional de Moneda i Timbre), CATCert (Catalunya).

Usos del certificat digital:

- DNI electrònic (DNIe).
- Certificat de persona física o jurídica.
- Signatura de correus electrònics (S/MIME).
- Connexió segura a webs de l'Administració pública.

Enginyeria social

L'**enginyeria social** és la manipulació psicològica dels usuaris per obtenir informació confidencial o accés a sistemes, sense necessitat de vulnerar cap sistema tècnic.

Tècniques habituals:

- **Phishing**: correu fals que simula ser una entitat legítima (banc, empresa).
- **Vishing**: mateixa tècnica per telèfon.
- **Smishing**: via SMS.
- **Baiting**: deixar un USB infectat perquè algú el connecti.

Defensa: formació i conscienciació dels usuaris. Cap sistema tècnic és suficient si l'usuari pot ser enganyat.

RA5 --- Legislació i Normativa

5.1. Protecció de dades: RGPD i LOPDGD

Marc normatiu

Nivell europeu:

- **RGPD** --- Reglament (UE) 2016/679: d'aplicació directa a tota la UE des del maig de 2018. Protegeix els drets i llibertats de les persones físiques en el tractament de les seves dades.
- **Directiva (UE) 2016/680**: regula dades tractades per autoritats per a finalitats penals.

Nivell espanyol:

- **Constitució espanyola (Article 18.4)**: garanteix la intimitat personal i familiar davant l'ús de la informàtica.
- **LOPDGD** --- Llei Orgànica 3/2018: adapta el dret espanyol al RGPD i estableix els drets digitals.
- **LSSI** --- Llei 34/2002: regula els serveis de la societat de la informació i el comerç electrònic.
- **Llei 25/2007**: obliga a retenir dades de trànsit de comunicacions electròniques.

Nivell català:

- **APDCAT** (Autoritat Catalana de Protecció de Dades): vetlla per la protecció de dades al sector públic de Catalunya.

Dades personals: definició

Qualsevol informació sobre una persona física **identificada o identificable**:

- Nom, cognoms, data de naixement, adreça.
- Adreça de correu electrònic, adreça IP.
- Empremtes dactilars, iris, dades genètiques.
- Orientació sexual, ideologia, creences religioses.
- Dades econòmiques, historial de consums.

> La protecció afecta **només persones físiques**, no empreses o persones jurídiques.

Categories especials (requereixen protecció reforçada): origen racial, afiliació sindical, opinions polítiques, salut, dades genètiques.

Figures responsables

Figura	Rol
Responsable del tractament	Persona/empresa que decideix les finalitats i mitjans del tractament. Ha de garantir el compliment del RGPD.
Encarregat del tractament	Empresa externa que tracta dades per compte del responsable, seguint les seves instruccions.
Delegat de Protecció de Dades (DPO)	Obligatori en organismes públics i empreses que tracten dades a gran escala. Assessora i supervisa el compliment.

Principis del RGPD

- **Responsabilitat proactiva** (*accountability*): demostrar activament el compliment.
- **Enfocament de risc**: les mesures s'adapten al risc real de cada tractament.
- **Minimització de dades**: recollir només el necessari per a la finalitat específica.
- **Qualitat**: dades exactes i actualitzades.
- **Registre d'activitats**: mantenir un registre intern dels tractaments (obligatori per a empreses de +250 treballadors o que tractin dades confidencials).

Drets de les persones (ARCO+)

- **Accés**: conèixer quines dades es tracten.
- **Rectificació**: corregir dades inexactes.
- **Supressió** ("dret a l'oblit"): eliminar les dades.
- **Oposició**: oposar-se al tractament en determinats casos.
- **Portabilitat**: rebre les dades en format reutilitzable.
- **Limitació**: restringir el tractament en certes circumstàncies.

Seguretat tècnica requerida

- Pseudonimització i xifratge de dades.
- Còpies de seguretat per garantir integritat i disponibilitat.
- Procediments de verificació periòdica de mesures de seguretat.
- Bloqueig de dades quan ja no siguin necessàries, però no puguin ser eliminades.

5.2. LSSI: comerç electrònic i correu

Àmbit d'aplicació

La **LSSI** (Llei 34/2002) s'aplica a qualsevol servei prestat a títol onerós, a distància i per via electrònica: comerç en línia, diaris digitals, motors de cerca, accés a la xarxa.

Obligacions dels prestadors de serveis

Deure d'informació: qualsevol web amb activitat econòmica ha de mostrar de forma permanent i gratuïta:

- Nom o denominació social i NIF.
- Domicili i adreça de correu electrònic.
- Dades d'inscripció registral o títols acadèmics (si escau).

Deure de col·laboració: han de col·laborar amb les autoritats per interrompre serveis o retirar continguts il·lícits.

Retenció de dades: han de retenir dades de trànsit de comunicacions fins a **12 mesos** per a investigacions judicials.

Comerç electrònic

- Els contractes electrònics són **vàlids i efectius** sense necessitat d'acord previ sobre l'ús de mitjans electrònics.
- **Informació precontractual**: l'usuari ha de conèixer el procés de contractació, arxiu del document, llengua del contracte.
- **Confirmació**: l'oferent ha de confirmar la recepció de l'acceptació en **24 hores**.

Correu comercial i spam

- **Prohibit** enviar comunicacions publicitàries per correu electrònic sense el **consentiment previ** del destinatari.
- *Excepció*: relació contractual prèvia amb productes similars, sempre que es permeti oposar-se fàcilment.
- Les comunicacions comercials han de ser clarament **identificables com a tals**.

Privadesa del correu electrònic

- El correu es considera equivalent a la correspondència privada i el **Codi Penal** protegeix contra la seva intercepció.
- A l'àmbit laboral, l'empresa pot controlar el correu corporatiu si hi ha normes d'ús prèviament establertes i acceptades pels treballadors, però **mai** pot accedir al correu personal.
- Per garantir la privadesa: usar **signatura digital** (autenticitat + integritat) i **xifratge** (confidencialitat).

Cookies

La normativa obliga a:

- Informar clarament sobre l'ús de cookies.
- Obtenir el **consentiment** de l'usuari (excepte cookies tècniques imprescindibles).
- Permetre que l'usuari accepti o rebutgi les cookies de forma granular.

Normes de gestió de la seguretat de la informació

ISO/IEC 27001: estàndard internacional per a sistemes de gestió de la seguretat de la informació (SGSI). Proporciona un marc sistemàtic per protegir informació confidencial.

Esquema Nacional de Seguretat (ENS): obligatori per a les administracions públiques espanyoles. Estableix els principis i requisits de seguretat dels sistemes d'informació públics.

Recursos addicionals

- **INCIBE**: https://www.incibe.es --- Telèfon d'ajuda: **017**
- **AEPD**: https://www.aepd.es --- Agència Espanyola de Protecció de Dades
- **APDCAT**: https://apdcat.cat --- Autoritat Catalana de Protecció de Dades
- **OSI**: https://www.incibe.es/ciudadania --- Oficina de Seguretat de l'Internauta
- **CCN-CERT**: https://www.ccn-cert.cni.es --- Centre Criptològic Nacional

Versions d'aquest document

- HTML - 0226.html
- PDF - 0226.pdf
- ODT - 0226.odt
- MD - 0226.md