
RA1. Adopció de pautes i pràctiques de tractament segur de la informació

Índex

Introducció	1
1. Adopció de pautes de seguretat informàtica	1
1.1 Fiabilitat, confidencialitat, integritat i disponibilitat	1
1.2 Elements vulnerables en el sistema informàtic	2
1.3 Anàlisi de les principals vulnerabilitats d'un sistema informàtic	2
1.4 Amenaces. Tipus: amenaces físiques i amenaces lògiques	3
2. Enginyeria social i fraus informàtics	3
Tècniques principals	4
Per què funciona?	4
Mesures de mitigació	4
3. Seguretat física i ambiental	5
Diferències entre seguretat física i lògica	5
Mesures de seguretat física	5
4. Seguretat lògica	5
4.1 Llistes de control d'accés (ACL)	5
4.2 Establiment de polítiques de contrasenyes	6
4.3 Polítiques d'emmagatzematge	6
4.4 Còpies de seguretat i imatges de suport	7
4.5 Mitjans d'emmagatzematge	7
5. Sistemes biomètrics	8
Tipus de sistemes biomètrics	8
Avantatges	8
Inconvenients i limitacions	8
6. Tècniques criptogràfiques	9
6.1 Xifratge simètric	9
6.2 Xifratge asimètric	9
6.3 Funcions de resum (hash)	10
6.4 Signatura digital	10
6.5 Xifratge en emmagatzematge i en trànsit	10
7. Protecció perimetral	10
Elements d'un pla de protecció perimètrica	11
Defensa en profunditat	11
8. Anàlisi forense en sistemes informàtics	11
Fases de l'anàlisi forense	12
Ordre de volatilitat	12
Referències i recursos complementaris	13

Introducció

Aquest document cobreix el primer resultat d'aprenentatge del mòdul de Seguretat i alta disponibilitat: adoptar pautes i pràctiques de tractament segur de la informació, reconeixent les vulnerabilitats d'un sistema informàtic i la necessitat d'assegurar-lo.

Es treballen els conceptes fonamentals de la seguretat informàtica (fiabilitat, confidencialitat, integritat i disponibilitat), les vulnerabilitats i amenaces d'un sistema, la seguretat física i lògica, l'enginyeria social, les polítiques de contrasenyes, la biometria, la criptografia, la protecció perimetral i l'anàlisi forense.

1. Adopció de pautes de seguretat informàtica

1.1 Fiabilitat, confidencialitat, integritat i disponibilitat

La seguretat informàtica no és un producte, és un **procés** continu. No existeix el "sistema 100% segur"; l'objectiu real és minimitzar el risc fins a un nivell acceptable i mantenir-lo controlat en el temps.

Es defineix la **fiabilitat** com la probabilitat que un sistema es comporti tal com s'espera d'ell. Aquesta fiabilitat es concreta en tres propietats clàssiques, conegudes com la **tríada CIA** (*Confidentiality, Integrity, Availability*):

- **Confidencialitat:** la informació només ha de ser accessible per a les persones, entitats o processos autoritzats. Es garanteix mitjançant control d'accés, xifratge i classificació de la informació.
- **Integritat:** la informació ha de mantenir-se exacta i completa, sense modificacions no autoritzades. S'implementa amb sumes de verificació (hash), signatures digitals, control de versions i permisos d'escriptura ben definits.
- **Disponibilitat:** la informació i els recursos han d'estar accessibles quan els usuaris autoritzats ho necessitin. Es treballa amb redundància de maquinari, còpies de seguretat, clústers d'alta disponibilitat i plans de contingència.

A aquestes tres propietats sovint se n'hi afegeixen dues més:

- **Autenticitat:** garantir que l'origen de la informació és qui diu ser (autenticació d'usuaris, certificats digitals).
- **No repudi:** impedir que l'emissor o el receptor d'una comunicació puguin negar haver-la realitzat (signatura digital, registres d'auditoria).

NOTA

Quan una empresa pateix un incident de seguretat, gairebé sempre es pot classificar segons quina d'aquestes propietats ha estat compromesa: una fuga de dades trenca la confidencialitat, un ransomware que xifra fitxers trenca la disponibilitat (i sovint també la integritat), i una manipulació de registres comptables trenca la integritat.

1.2 Elements vulnerables en el sistema informàtic

Un sistema informàtic no és només l'ordinador: cal entendre'l com un conjunt d'elements interrelacionats, cadascun amb les seves pròpies vulnerabilitats.

Maquinari (hardware)

- Fallades físiques: avaries de disc, sobreescalfament, talls d'alimentació.
- Robatori o accés físic no autoritzat a equips i servidors.
- Desastres naturals: incendis, inundacions, terratrèmols.
- Manipulació física de dispositius (keyloggers de maquinari, dispositius USB maliciosos).

Programari (software)

- Errors de programació (*bugs*) que deriven en vulnerabilitats explotables.
- Sistemes operatius o aplicacions sense actualitzar (*patches* de seguretat pendents).
- Configuracions per defecte insegures (contrasenyes d'administrador sense canviar, serveis innecessaris actius).
- Programari maliciós: virus, cucs, troians, ransomware, spyware.

Dades

- Accés no autoritzat a informació confidencial.
- Pèrdua de dades per esborrament accidental o intencionat.
- Alteració de dades sense detecció.
- Fuga d'informació confidencial (intencionada o per negligència).

Element humà

- Sovint és la baula més feble de la cadena: manca de formació, errors involuntaris, o accions malintencionades d'usuaris interns.

1.3 Anàlisi de les principals vulnerabilitats d'un sistema informàtic

Una **vulnerabilitat** és una debilitat en un actiu que pot ser explotada per una amenaça. Es poden classificar segons diversos criteris:

Segons l'origen:

Tipus	Descripció	Exemples
Disseny	Errors en l'especificació o disseny del protocol/sistema	Debilitats de TCP/IP, protocols sense xifratge (Telnet, FTP)
Implementació	Errors en la codificació d'un programa	Buffer overflow, injecció SQL, XSS
Ús/configuració	Configuració incorrecta o ús inadequat	Contrasenyes per defecte, ports oberts innecessaris, permisos excessius

Segons la tipologia:

- **Vulnerabilitats de programari:** errors en aplicacions o sistemes operatius (CVE publicades a bases de dades com NVD).
- **Vulnerabilitats de xarxa:** protocols insegurs, absència de segmentació, punts d'accés wifi mal protegits.

- **Vulnerabilitats físiques:** accés no controlat a sales de servidors, manca de vigilància.
- **Vulnerabilitats humanes:** manca de formació, susceptibilitat a l'enginyeria social.

1.4 Amenaces. Tipus: amenaces físiques i amenaces lògiques

Mentre que la vulnerabilitat és una debilitat del sistema, l'**amenança** és qualsevol circumstància o esdeveniment amb el potencial de causar dany explotant aquesta vulnerabilitat.

Amenaces físiques

- Naturals: incendis, inundacions, terratrèmols, talls elèctrics.
- Ambientals: pols, humitat, temperatura inadequada a les sales de servidors.
- Robatori o sabotatge d'equips.
- Accés físic no autoritzat.

Amenaces lògiques

- **Programari maliciós (malware):** virus, cucs (*worms*), troians, ransomware, spyware, adware.
- **Atacs de xarxa:** sniffing, spoofing, man-in-the-middle, denegació de servei (DoS/DDoS).
- **Atacs a aplicacions web:** injecció SQL, cross-site scripting (XSS), cross-site request forgery (CSRF).
- **Enginyeria social:** phishing, pretexting, baiting (es tracta en detall a l'apartat 2).
- **Amenaces internes:** usuaris legítims que abusen dels seus privilegis, intencionadament o no.

També es distingeix entre:

- **Amenaces intencionades:** atacants amb un objectiu concret (robar dades, extorsionar, sabotejar).
- **Amenaces no intencionades:** errors humans, fallades tècniques sense intenció malintencionada.

2. Enginyeria social i fraus informàtics

L'enginyeria social consisteix a manipular psicològicament les persones perquè revelin informació confidencial o realitzin accions que comprometin la seguretat, explotant la confiança, la por o la urgència en lloc de vulnerabilitats tècniques.

Tècniques principals

- **Phishing:** correus electrònics fraudulents que simulen procedir d'una entitat legítima (banc, empresa, administració) per obtenir credencials o dades bancàries.
- **Spear phishing:** variant dirigida a una persona o organització concreta, amb informació personalitzada que augmenta la credibilitat.
- **Vishing:** phishing per veu telefònica, sovint suplantant suport tècnic o entitats bancàries.
- **Smishing:** phishing mitjançant missatges SMS.
- **Pretexting:** l'atacant crea una situació o identitat falsa (per exemple, fer-se passar per tècnic informàtic) per obtenir informació.
- **Baiting:** deixar un dispositiu infectat (per exemple, un llapis de memòria) en un lloc visible perquè algú el connecti per curiositat.
- **Shoulder surfing:** observar directament per sobre l'espatlla d'algú mentre introdueix una contrasenya o dades confidencials.
- **Tailgating/piggybacking:** seguir físicament una persona autoritzada per accedir a una zona restringida sense credencials pròpies.

Per què funciona?

L'enginyeria social explota principis psicològics ben coneguts: autoritat (fer-se passar per un càrrec superior o un tècnic), urgència (crear pressió temporal per evitar la reflexió), confiança social i por a les conseqüències.

Exemple pràctic d'aula: mostra als estudiants un correu de phishing real (anonimitzat) i demana'ls que identifiquin els indicadors d'alarma: domini del remitent sospitos, enllaços que no coincideixen amb el text visible, faltes ortogràfiques, sensació d'urgència, sol·licitud de dades que l'entitat legítima mai demanaria per correu.

Mesures de mitigació

- Formació i conscienciació contínua dels usuaris (és la mesura més efectiva).
- Verificació de la identitat per un canal alternatiu abans d'actuar sobre peticions confidencials.
- Filtres antiphishing i antispam als servidors de correu.
- Polítiques clares sobre quina informació mai es demana per telèfon o correu.
- Simulacres de phishing controlats per mesurar i millorar la resposta dels usuaris.

3. Seguretat física i ambiental

Diferències entre seguretat física i lògica

Aspecte	Seguretat física	Seguretat lògica
Protegeix	El maquinari, les instal·lacions, l'entorn	Les dades, els accessos, els processos
Amenaces típiques	Robatori, incendi, inundació, accés físic no autoritzat	Malware, atacs de xarxa, accés no autoritzat a dades
Mesures	Control d'accés físic, CCTV, SAI, climatització, extinció d'incendis	Contrasenyes, xifratge, tallafocs, ACL, antivirus

Ambdues són complementàries: de res serveix un sistema amb el millor xifratge del món si qualsevol persona pot entrar físicament a la sala de servidors i endur-se el disc dur.

Mesures de seguretat física

- **Control d'accés:** targetes, claus, sistemes biomètrics a les portes de les sales de servidors (CPD).
- **Videovigilància (CCTV):** registre i dissuasió d'accessos no autoritzats.
- **Control ambiental:** climatització per evitar sobreescalfament, control d'humitat.
- **Sistemes d'alimentació ininterrompuda (SAI/UPS):** protecció davant talls elèctrics.
- **Sistemes d'extinció d'incendis:** detectors de fum i sistemes d'extinció adequats per a equipament electrònic (gasos inerts, no aigua).
- **Ubicació del CPD:** evitar plantes baixes en zones inundables, evitar visibilitat exterior de la ubicació dels servidors.

4. Seguretat lògica

4.1 Llistes de control d'accés (ACL)

Les **ACL (Access Control Lists)** defineixen quins usuaris o processos tenen permís per accedir a un recurs i quin tipus d'operacions poden fer-hi (lectura, escriptura, execució).

Es basen en el principi de **mínim privilegi**: cada usuari o procés ha de tenir només els permisos estrictament necessaris per fer la seva feina, ni més ni menys.

Exemple en Linux (ACL sobre el sistema de fitxers):

```
# Consultar les ACL d'un fitxer
getfacl /var/www/dades_confidencials.txt

# Donar permís de lectura a un usuari concret sense afectar el grup
setfacl -m u:alumne1:r-- /var/www/dades_confidencials.txt

# Donar permís de lectura/escriptura a un grup
setfacl -m g:professors:rw- /var/www/dades_confidencials.txt

# Eliminar totes les ACL d'un fitxer
```

```
setfacl -b /var/www/dades_confidencials.txt
```

4.2 Establiment de polítiques de contrasenyes

Una política de contrasenyes robusta és una de les mesures de seguretat lògica més bàsiques i alhora més sovint descuidades.

Característiques d'una contrasenya robusta:

- Longitud mínima recomanada: 12-14 caràcters (millor com més llarga).
- Combinació de majúscules, minúscules, xifres i símbols.
- Absència de paraules de diccionari, dades personals (dates de naixement, noms) o patrons previsibles (123456, qwer ty).
- Única per a cada servei (evitar la reutilització).

Elements d'una política de contrasenyes corporativa:

- Longitud i complexitat mínimes obligatòries.
- Caducitat periòdica (encara que les recomanacions actuals com les del NIST tendeixen a prioritzar la longitud i l'ús de gestors de contrasenyes per sobre de canvis forçats molt freqüents).
- Historial de contrasenyes (impedir reutilitzar les últimes N contrasenyes).
- Bloqueig de compte després d'un nombre determinat d'intents fallits.
- Autenticació multifactor (MFA) com a capa addicional, especialment per a comptes d'administració.

4.3 Polítiques d'emmagatzematge

Fan referència a com, on i durant quant de temps es guarda la informació, en funció de la seva sensibilitat:

- **Classificació de la informació:** pública, interna, confidencial, restringida.
- **Xifratge en repòs:** dades confidencials emmagatzemades de manera xifrada (BitLocker a Windows, LUKS a Linux).
- **Control d'accés diferenciat** segons el nivell de classificació.
- **Retenció i eliminació segura:** definir quant de temps es conserva la informació i com s'elimina de manera irreversible quan ja no és necessària (esborrament segur amb eines com shred a Linux).

4.4 Còpies de seguretat i imatges de suport

Les còpies de seguretat (*backups*) són la mesura més important per garantir la disponibilitat i la recuperació davant incidents (ransomware, fallades de maquinari, errors humans).

Tipus de còpies de seguretat:

Tipus	Descripció	Avantatges	Inconvenients
Completa	Còpia de tota la informació	Restauració senzilla i ràpida	Ocupa molt d'espai, triga més
Incremental	Còpia només dels canvis des de l'última còpia (de qualsevol mena)	Ràpida, ocupa poc espai	Restauració més lenta (cal aplicar totes les incrementals)
Diferencial	Còpia dels canvis des de l'última còpia completa	Restauració més ràpida que la incremental	Ocupa més espai que la incremental amb el temps

Regla 3-2-1, un estàndard de referència en la planificació de còpies de seguretat:

- **3** còpies de les dades (l'original més 2 còpies).
- **2** suports d'emmagatzematge diferents.
- **1** còpia fora de les instal·lacions (*offsite*), idealment desconnectada de la xarxa (protecció davant ransomware).

Imatges de suport (*disk images*): a diferència d'una còpia de seguretat de fitxers, una imatge de disc captura l'estat complet d'un sistema (sistema operatiu, aplicacions, configuració i dades), cosa que permet una restauració completa en cas de fallada greu. Eines com **Clonezilla** o **FOG Server** permeten crear i desplegar imatges de suport en entorns d'aula.

4.5 Mitjans d'emmagatzematge

La tria del mitjà d'emmagatzematge també té implicacions de seguretat:

- **Discs durs (HDD) i SSD:** cal considerar el xifratge i l'esborrament segur en donar-los de baixa.
- **Emmagatzematge en xarxa (NAS/SAN):** centralitza les dades, facilita la gestió de permisos i les còpies de seguretat, però requereix protegir bé l'accés a la xarxa.
- **Emmagatzematge extraïble (USB, discs externs):** còmode, però amb alt risc de pèrdua, robatori o introducció de malware; cal establir polítiques d'ús restrictives.
- **Emmagatzematge al núvol:** cal valorar la ubicació geogràfica de les dades (aspectes legals, RGPD), el xifratge en trànsit i en repòs, i la fiabilitat del proveïdor.

5. Sistemes biomètrics

La **biometria** utilitza característiques físiques o de comportament úniques d'una persona per a l'autenticació, substituint o complementant les contrasenyes.

Tipus de sistemes biomètrics

Biometria física:

- Empremta dactilar.
- Reconeixement facial.
- Iris o retina.
- Geometria de la mà.

Biometria de comportament:

- Reconeixement de veu.
- Patró de signatura manuscrita.
- Dinàmica de tecleig (*keystroke dynamics*).

Avantatges

- No es pot oblidar, perdre ni compartir amb la mateixa facilitat que una contrasenya.
- Díficil de falsificar (encara que no impossible).
- Millora l'experiència d'usuari (autenticació ràpida, sense necessitat de recordar credencials).
- Molt adequada per combinar-se amb altres factors en un esquema MFA (allò que ets + allò que saps + allò que tens).

Inconvenients i limitacions

- Un cop compromesa una dada biomètrica (per exemple, una empremta filtrada en una fuga de dades), no es pot "canviar" com una contrasenya.
- Cost d'implementació més elevat que un sistema de contrasenyes tradicional.
- Possibles falsos positius/negatius (taxa FAR i FRR).
- Implicacions de privadesa: les dades biomètriques són dades personals especialment protegides pel RGPD.

6. Tècniques criptogràfiques

La criptografia permet protegir la confidencialitat i la integritat de la informació, tan emmagatzemada com en trànsit.

6.1 Xifratge simètric

Utilitza la mateixa clau per xifrar i desxifrar. És ràpid i eficient per a grans volums de dades, però requereix un mètode segur per compartir la clau entre les parts.

- Algorismes habituals: **AES** (Advanced Encryption Standard, l'estàndard actual), 3DES (en desús).

```
# Xifrar un fitxer amb AES-256 utilitzant OpenSSL
openssl enc -aes-256-cbc -salt -pbkdf2 -in document_confidencial.txt
↪ -out document.enc

# Desxifrar el fitxer
openssl enc -aes-256-cbc -d -pbkdf2 -in document.enc -out
↪ document_confidencial.txt
```

6.2 Xifratge asimètric

Utilitza un parell de claus matemàticament relacionades: una **clau pública** (es pot compartir lliurement) i una **clau privada** (s'ha de mantenir secreta). El que xifra una clau, només ho pot desxifrar l'altra.

- Algorismes habituals: **RSA**, **ECC** (criptografia de corba el·líptica).
- És més lent que el simètric, per això sovint s'utilitza per intercanviar de manera segura una clau simètrica (xifratge híbrid, com fa TLS).

```
# Generar un parell de claus RSA
openssl genpkey -algorithm RSA -out clau_privada.pem -pkeyopt
↪ rsa_keygen_bits:4096
openssl rsa -pubout -in clau_privada.pem -out clau_publica.pem

# Xifrar amb la clau pública del destinatari
openssl pkeyutl -encrypt -pubin -inkey clau_publica.pem -in
↪ missatge.txt -out missatge.enc

# Desxifrar amb la clau privada
openssl pkeyutl -decrypt -inkey clau_privada.pem -in missatge.enc -out
↪ missatge_desxifrat.txt
```

6.3 Funcions de resum (hash)

Generen una empremta digital de longitud fixa a partir d'unes dades d'entrada de qualsevol mida. No són reversibles i qualsevol canvi mínim a l'entrada produeix un resultat completament diferent. S'utilitzen per verificar la integritat i per emmagatzemar contrasenyes de manera segura (mai en clar).

- Algorismes recomanats actualment: **SHA-256, SHA-3**.
- **MD5 i SHA-1 estan obsolets** per a usos de seguretat (col·lisions demostrades) tot i que encara s'usen per a verificacions d'integritat no crítiques.
- Per emmagatzemar contrasenyes: mai un hash simple, sinó funcions específiques amb *salt* i cost computacional ajustable, com **bcrypt**, **scrypt** o **Argon2**.

```
# Calcular el hash SHA-256 d'un fitxer
sha256sum informe.pdf

# Verificar la integritat comparant amb un hash conegut
echo "hash_esperat informe.pdf" | sha256sum -c -
```

6.4 Signatura digital

Combina el hash i la criptografia asimètrica per garantir alhora la integritat, l'autenticitat i el no repudi d'un document o missatge: l'emissor xifra el hash del document amb la seva clau privada, i qualsevol receptor pot verificar-ho amb la clau pública corresponent.

6.5 Xifratge en emmagatzematge i en trànsit

- **En repòs (*at rest*)**: xifratge de disc complet (BitLocker, LUKS/dm-crypt), xifratge de fitxers o carpetes concretes, xifratge a escala de base de dades.
- **En trànsit (*in transit*)**: TLS/SSL per a comunicacions web (HTTPS), SSH per a administració remota, VPN (com WireGuard) per xifrar tot el trànsit entre xarxes.

7. Protecció perimetral

Un **pla integral de protecció perimètrica** és especialment crític en sistemes connectats a xarxes públiques (Internet), on l'exposició a amenaces externes és molt superior.

Elements d'un pla de protecció perimètrica

- **Tallafocs (firewall)**: filtra el trànsit entre la xarxa interna i l'externa segons regles definides. Pot ser de xarxa (a escala de perímetre) o d'amfitrió (en cada equip).
- **Zona desmilitaritzada (DMZ)**: segment de xarxa aïllat on es col·loquen els serveis que han de ser accessibles des d'Internet (servidor web, correu), separant-los de la xarxa interna per limitar l'impacte d'un compromís.
- **Sistemes de detecció i prevenció d'intrusions (IDS/IPS)**: monitoren el trànsit per detectar (IDS) o bloquejar activament (IPS) patrons d'atac coneguts.
- **VPN**: permet l'accés remot segur a la xarxa interna mitjançant un túnel xifrat.
- **Segmentació de xarxa (VLAN)**: divideix la xarxa en segments lògics per limitar la propagació d'un incident.
- **Proxy invers i balancejadors de càrrega**: com HAProxy, afegeixen una capa addicional entre l'usuari extern i els servidors reals, ocultant-ne la topologia.

Defensa en profunditat

El concepte de **defensa en profunditat** (*defense in depth*) proposa no confiar en una única mesura de seguretat, sinó establir múltiples capes independents, de manera que si una falla, les altres continuïn protegint el sistema:



8. Anàlisi forense en sistemes informàtics

L'**anàlisi forense digital** és el procés d'identificar, preservar, analitzar i presentar evidències digitals després d'un incident de seguretat, amb l'objectiu de determinar què ha passat, com ha passat i, si escau, qui n'és responsable, mantenint sempre la validesa de les proves des d'un punt de vista legal.

Fases de l'anàlisi forense

1. **Identificació** Detectar que s'ha produït un incident i identificar quins sistemes, dispositius o dades poden contenir evidències rellevants.
2. **Preservació** Garantir que les evidències no es contaminen ni es modifiquen. Es treballa sempre sobre còpies exactes (imatges forenses bit a bit), mai sobre el sistema original, i es documenta la **cadena de custòdia**: qui ha tingut accés a l'evidència, quan i per què.

```
# Crear una imatge forense d'un dispositiu amb dd, calculant el  
↪ hash per verificar-ne la integritat  
dd if=/dev/sdb of=/evidencies/disc_incident.img bs=4M  
↪ status=progress  
sha256sum /dev/sdb /evidencies/disc_incident.img
```

3. **Anàlisi** Examinar les evidències preservades per reconstruir els fets: anàlisi de registres (logs), recuperació de fitxers esborrats, anàlisi de la memòria RAM (memòria volàtil, s'ha de capturar abans d'apagar l'equip si és possible), línia temporal (*timeline*) d'esdeveniments.
4. **Documentació** Registrar detalladament totes les accions realitzades, les eines utilitzades i els resultats obtinguts, de manera reproduïble.
5. **Presentació** Elaborar un informe clar i comprensible (tècnicament rigorós però adaptat al destinatari, que pot no ser tècnic) amb les conclusions de l'anàlisi, apte per a un context intern o, si escau, judicial.

NOTA

Un principi fonamental de l'anàlisi forense és **no alterar mai l'evidència original**. Per això sempre es treballa sobre còpies, es documenta cada pas i es verifica la integritat amb funcions hash abans i després de cada manipulació.

Ordre de volatilitat

En capturar evidències, cal seguir l'**ordre de volatilitat**, recollint primer allò que es perd més ràpidament:

1. Registres de la CPU, memòria cau.
2. Memòria RAM (contingut de processos en execució, connexions de xarxa actives).
3. Estat de la xarxa (connexions actives, taules de rutes).
4. Processos en execució.
5. Sistema de fitxers i discos.
6. Registres (*logs*) del sistema.
7. Configuració física i topologia de xarxa.
8. Suports de backup.

Referències i recursos complementaris

- [NIST SP 800-63B --- Digital Identity Guidelines \(polítiques de contrasenyes\)](#)
- [INCIBE --- Contraseñas seguras](#) (equivalent en castellà, orientat a ciutadania i empresa)
- [NVD --- National Vulnerability Database](#)
- [INCIBE-CERT --- Vulnerabilidades](#) (traducció al castellà de la NVD, +75.000 CVE)
- [OWASP Top 10](#)
- [INCIBE-CERT --- OWASP publica el Top 10 de riesgos en aplicaciones web](#) (difusió i anàlisi en castellà; INCIBE no en publica una llista pròpia)

Versions d'aquest document

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

[Domini Públic \(CC0\)](#)