Seguretat física, lògica i legislació

UF1

M11 Seguretat i alta diponibilitat

CURS 2015 - 2016

Hèctor López
hector.lopez@fje.edu

JESUÏTES El Clot
Escola del Clot

Introducció a la Seguretat

Què és la seguretat informàtica?

- Conjunt de tècniques i polítiques que tracten de minimitzar la vulnerabilitat dels **sistemes** o de la **informació** que contenen.
- Es tracta d'aconseguir que el cost d'aconseguir accedir a un recurs de forma indeguda sigui més alt que el seu valor.
- La seguretat és un **procés** no un producte.
- La seguretat total no existeix.

Introducció a la Seguretat

Tipus de seguretat

Podem parlar de dos tipus de seguretat, que es complementen:

- **Seguretat física**: referent a la protecció dels components del sistema (hardware) davant les amenaces físiques: incendis, inundacions, control d'accés de persones, caigudes del subministrament elèctric...

- **Seguretat lògica**: referent a la protecció de les dades. Les principals tècniques aplicades són el control d'accés i la criptografia

La gestió global de la seguretat d'una organització, com us podeu imaginar, ha de tractar els dos tipus de seguretat.

Introducció a la Seguretat

Tipus de seguretat

Quan es parla de seguretat informàtica es tendeix a pensar en tallafocs, antivirus, detectors i altres eines molt utilitzades en el món de la seguretat, però es tenen **menys presents** els conceptes relacionats amb la **seguretat física**.

El fet de decidir de manera encertada les característiques de la seguretat física, representa tenir una **base sòlida** sobre la qual construir els altres elements de seguretat.

Introducció a la Seguretat

Objectius de la seguretat

La seguretat té com a principals objectius, tot tenint en compte els principals components del sistema (hardware, software i dades):

- **Confidencialitat**: Els components del sistema només seran accessibles per usuaris autoritzats.
- **Integritat**: Els components del sistema només poden ser creats i modificats per usuaris autoritzats.
- **Disponibilitat**: Els components del sistema han d'estar accesibles als usuaris autoritzats.
- **No repudi**: referent a la comunicació entre un emissor in un receptor (client-servidor); en aquesta comunicació el receptor d'un missatge obté una prova vàlida davant un tercer de l'origen de les dades rebudes.

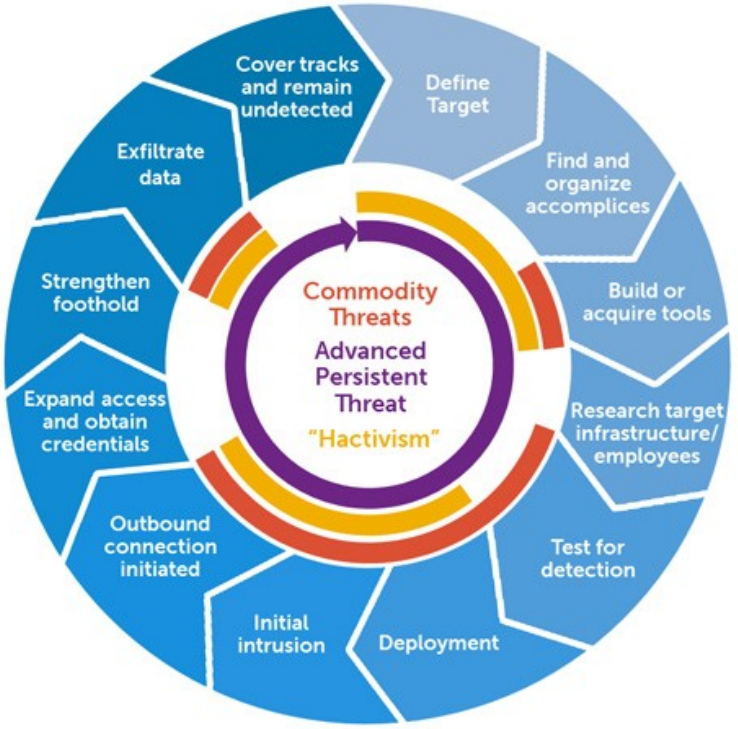
Introducció a la Seguretat

Amenaces

Les amenaces afecten principalment al **hardware**, al **software** i a les **dades**. Aquests son els tres **punts dèbils** de tot sistema.

Les amenaces provoquen fenòmens de:

- **Interrupció**
- **Interceptació**
- **Modificació**
- **Generació**



Introducció a la Seguretat

Tipus d'amenaces

- **Interrupció:** Un punt del sistema deixa de funcionar.

ex: destrucció de maquinari, fallada del sistema operatiu...

- **Interceptació:** Accés a la informació per part d' usuaris no autoritzats.

ex: les escoltes de la xarxa amb sniffers.

- **Modificació:** Accés no autoritzat que modifica l'entorn pel seu benefici.

ex: modificació de registres d'una base de dades, modificació de paquets TCP enviats per la xarxa.

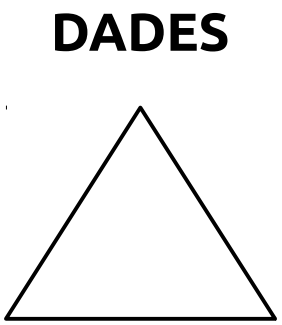
- **Generació**: Creació de nous objectes dins el sistema.

ex: crear nous registres en una base de dades.

Introducció a la Seguretat

Triangle de debilitats

Interrupció	Interceptació	Modificació	Generació
(pèrdua de dades)	(accés)	(canvi d'un reg)	(inserció d'un reg)



HARDWARE

- Interrupció (DoS)
- Interceptació (robatori)

SOFTWARE

- Interrupció (esborrat)
- Interceptació (còpia)
- Modificació (falsificació)

Introducció a la Seguretat

Altres classificacions d'amenaces (I)

Amenaces físiques → **Seguretat física**

- Temperatura ambiental.
- Caigudes del subministrament elèctric.
- Robatoris i desastres naturals.

Amenaces lògiques → **Seguretat lògica** (dades)

- Accés no autoritzat a les dades (**privacitat**)
- Lectura no autoritzada en la transmissió (**confidencialitat**).
- Modificació de dades durant la seva transmissió per un tercer actor no autorizat (**integritat**).
- **Suplantació** de la identitat d'un usuari.
- Denegació de serveis (**disponibilitat**).

Altres classificacions d'amenaces (II)

Una altra classificació de les amenaces, basada en la provinença de l'atac:

- Amenaces **internes**: ocasionades per agents interns a l'organització, per exemple els mateixos empleats, de manera conscient o inconscient.
- Amenaces **externes**: ocasionades per agents aliens a l'organització que a priori no tenen un coneixement intern dels sistemes, per exemple un hacker maliciós.

En principi les amenaces **internes** son **més perilloses** que les externes pel coneixement i el grau d'accés dels empleats al sistema.

Hèctor López
hector.lopez@fje.edu

Introducció a la Seguretat

Gestió de la seguretat

Assegurar un sistema informàtic és un tasca molt complexa que mai pot arribar a ser perfecta i s'ha d'analitzar amb molta cura **segons les necessitats** de l'organització **i els recursos** que es poden destinar a aquest objectiu.

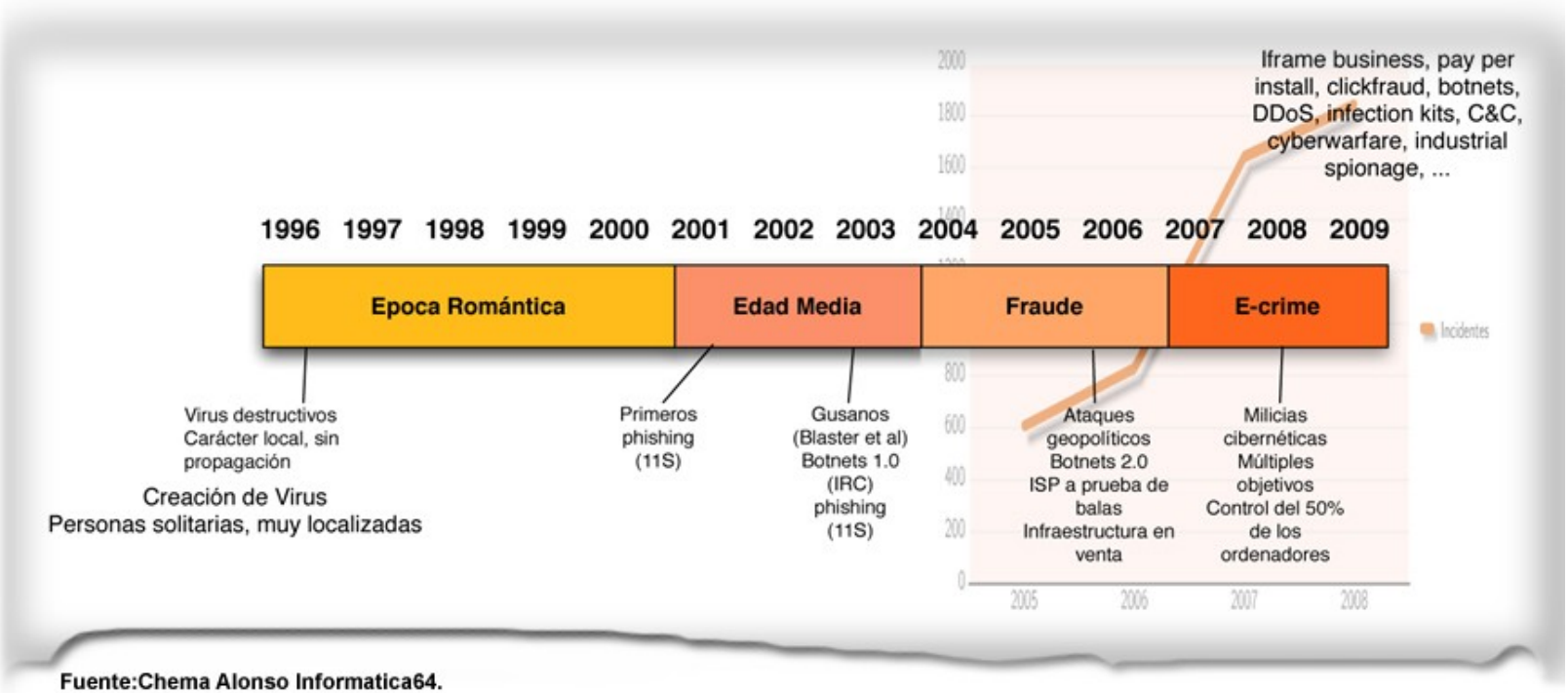
Els passos generals a seguir son els següents:

- Anàlisi dels **riscs** i les **amenaces**.
- Definició d'un **pla de seguretat** per minimitzar les amenaces.
- **Desplegar** la seguretat i **monitoritzar** el sistema.

Seguretat = Procés

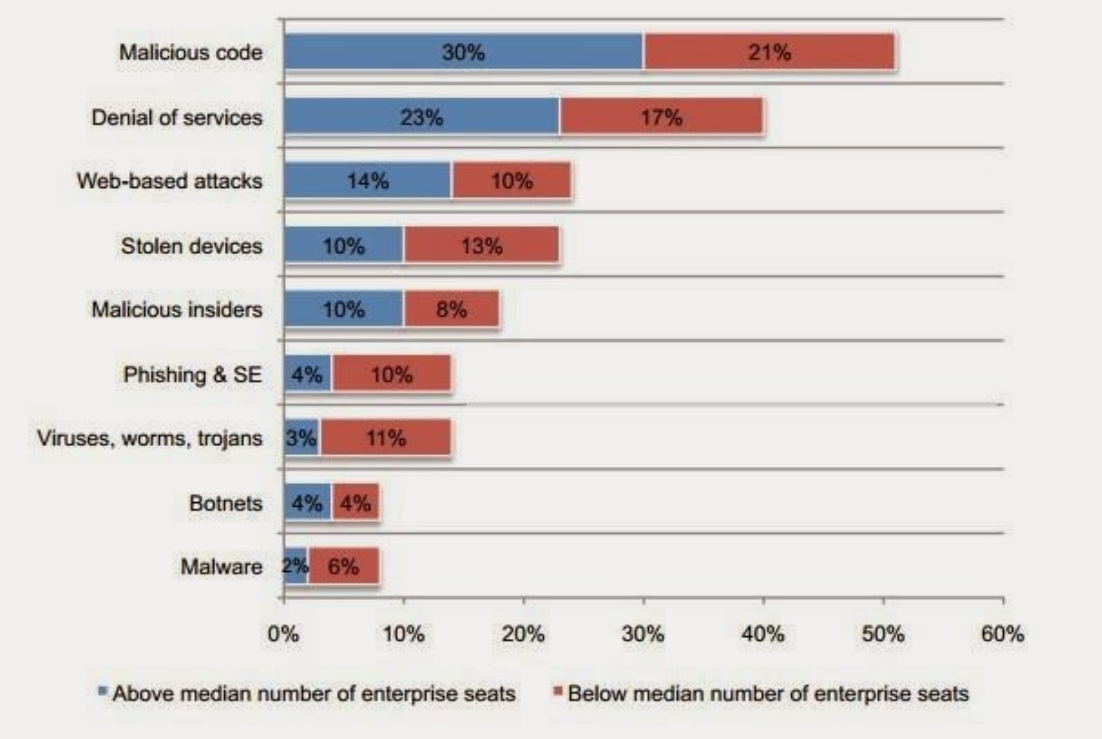
Introducció a la Seguretat

Evolució dels atacs informàtics (I)

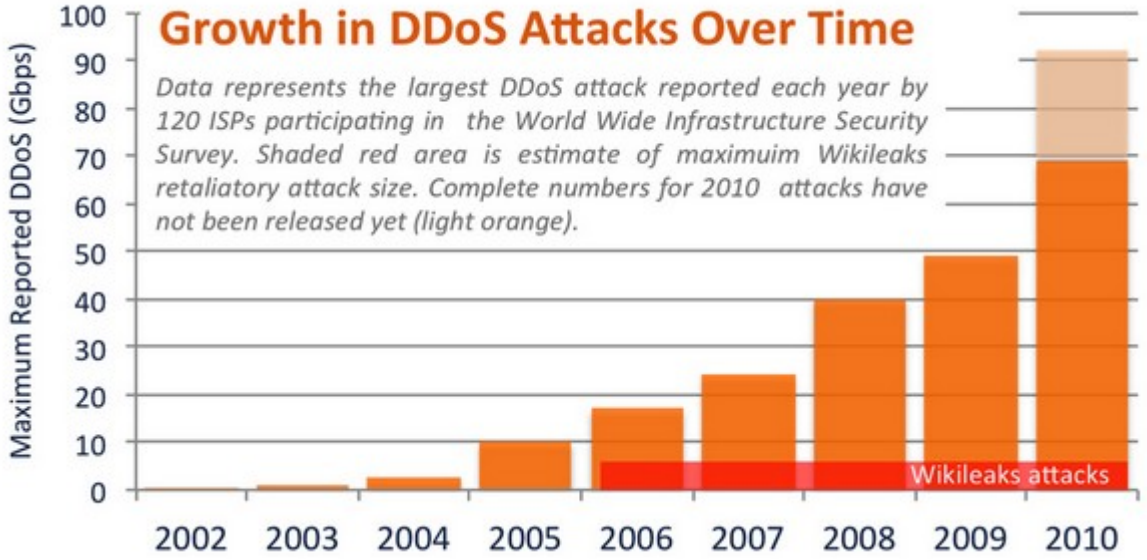


Fuente:Chema Alonso Informatica64.

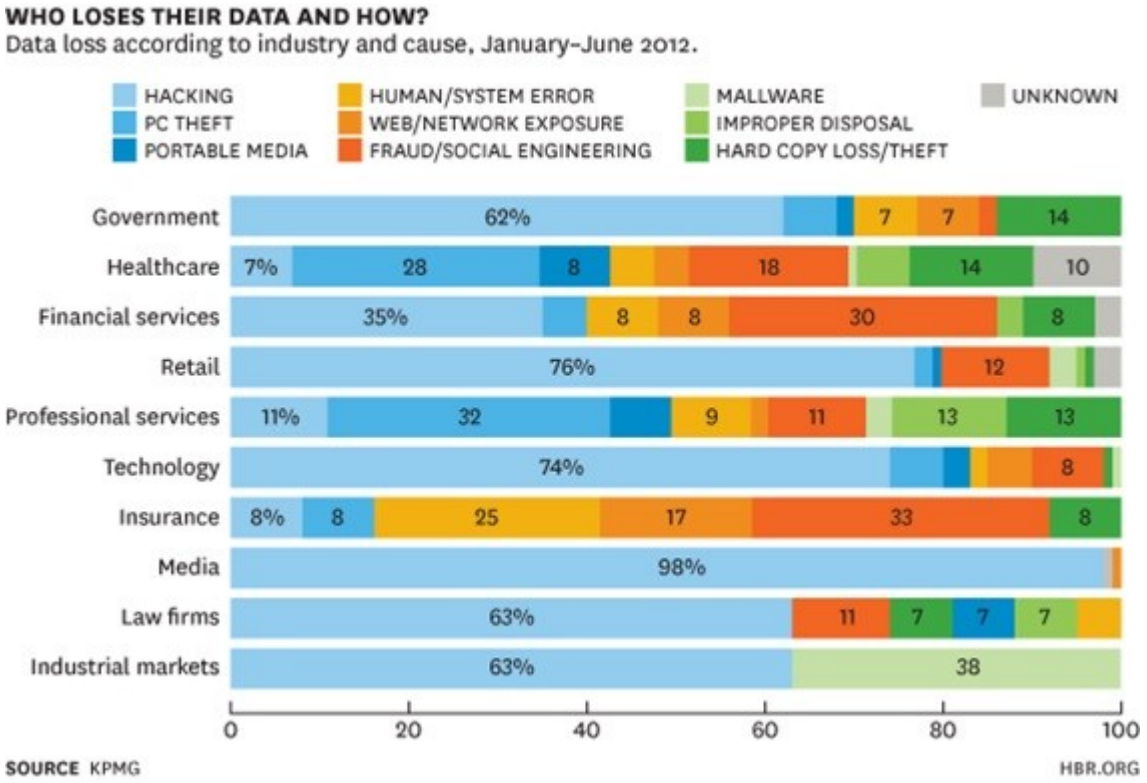
Evolució dels atacs informàtics (II)



Evolució dels atacs informàtics (III)



Evolució dels atacs informàtics (IV)



Introducció a la Seguretat

Classificació de les amenaces segons tipus d'atacants (I)

Un sistema informàtic està exposat a múltiples amenaces i atacs. A continuació una classificació de les amenaces segons el tipus d'atacants:

- **Hacker**: expert informàtic amb una gran capacitat per descobrir les vulnerabilitats dels sistemes, però sense motivació econòmica.
- **Cracker:** un hacker que, quan trenca la seguretat d'un sistema, ho fa amb la intenció o bé de danyarel sistema, o bé d'obtenir un reconeixement i/o benefici econòmic.
- **Lammer o Script-Kiddies:** pretenen fer hacking sense tenir coneixements avançats d'informàtica. Habitualment només es dediquen a buscar i descarregar programes de hacking per després executar-los.

Classificació de les amenaces segons tipus d'atacants (II)

Un sistema informàtic està exposat a múltiples amenaces i atacs. A continuació una classificació de les amenaces segons el tipus d'atacants:

- **Sniffers**: experts en xarxes que analitzen el trànsit per obtenir informació. Extreuen la informació dels paquets que es transmeten per la xarxa.
- **Programadors de virus:** experts en programació, xarxes, i sistemes que creen programes que danyen el sistema.

Seguretat lògica

Control d'accés

El **control d'accés**: és un mecanisme per garantir la seguretat de la informació.

→ Serveix per per especificar qui o què pot accedir a cadascun dels recursos del sistema, i també el tipus d'accés que se li permet en cada cas.

Hi ha dues funcions o processos principals per garantir el control d'accés:

- **Autenticació**: verificació de la identitat d'un usuari o d'una altra entitat del sistema.
- **Autorització:** la concessió d'un dret o d'un permís a una entitat del sistema per accedir a un recurs del sistema.

Seguretat lògica

Control d'accés

Terminologia

Un **objecte** és un recurs que té l'accés controlat.

→ Per exemple: registres, pàgines de memòria, fitxers, directoris I programes.

Un **subjecte** és una entitat capaç d'accedir a objectes.

→ En general el concepte de subjecte va lligat al de procés. Quan un usuari o aplicació vol accedir a un objecte, en realitat ho fa per mitjà d'un procés que representa l'usuari. Tot i així, és habitual parlar d'usuaris com a subjectes.

Seguretat lògica

Control d'accés

Sistemes GNU/Linux

En sistemes **GNU/Linux** hi ha tres classes de subjecte:

- Propietari
- Grup
- Altres

Un **dret d'accés** indica de quina manera un subjecte pot accedir a un objecte.

→ Per exemple: escriptura, lectura, execució.

Seguretat lògica

Control d'accés

Matrius i ACL

Les **matrius** són una possible implementació del control d'accés.

Exemple:

Subjectes	Objectes		
	/home/albert	/home/berta	/home/carme
Albert	Lectura, escriptura, cd		
Berta		Lectura, escriptura, cd	
Carme	Lectura, escriptura, cd	Lectura, escriptura, cd	Lectura, escriptura, cd

A la pràctica, la matriu de control d'accés es descompon en estructures més senzilles i manejables anomenades **ACL** (Access Control Lists). Per això es descompon la matriu en columnes i s'associa a cada objecte una llista de qui hi pot interactuar i com.

Seguretat lògica

Control d'accés

Autenticació (I)

Perquè un usuari accedeixi a un recurs d'un sistema cal que prèviament:

- Demostri que és qui diu que és (identificació).
- Tingui les credencials necessàries.
- Se li hagin donat els drets o privilegis (tant en termes d'accés, com per dur a terme les accions que demana).

La **identificació** és una manera d'assegurar-se que un subjecte (usuari o procés) és l'entitat que diu que és.

Control d'accés

Autenticació (II)

Determinar la identitat en seguretat informàtica té tres aspectes clau:

- **Unicitat:** en un sistema cada individu ha de tenir un identificador únic.
- **No descriptiva:** cap part de la credencial no ha d'indicar la finalitat del compte. Per exemple, un identificador d'usuari no hauria de ser webadmin, superusuari o gerent.
- **Expedició**: els elements proveïts per una altra autoritat reconeguda per demostrar la identitat d'un subjecte. El document nacional d'identitat és un tipus d'element de seguretat que es consideraria una forma d'expedició d'identificació.

Control d'accés

Autenticació (III)

Un cop el subjecte s'ha identificat, cal que s'autentiqui, és a dir, cal que demostrique és qui diu que és. Hi ha tres factors que s'utilitzen per a l'autenticació:

- Alguna cosa que una persona sap (**autenticació per coneixement**).
- Alguna cosa que una persona té (**autenticació per possessió**)
- Alguna cosa que una persona és o fa (**autenticació per característica**).

Hèctor López
hector.lopez@fje.edu

Control d'accés

Autenticació (IV)

Una **autenticació multifactor** utilitza dos o tres factors d'autenticació i assegura un nivell més alt de seguretat. En general, el tipus d'autenticació multifactor més utilitzada és l'autenticació de dos factors.

Un exemple:

→ un usuari vol accedir a un sistema i per fer-ho ha d'indicar alguna cosa que sap (contrasenya) i utilitzar alguna cosa que té (targeta magnètica).

→ una altra possibilitat podria ser una contrasenya més un atribut físic (escaneig de la retina).

Hèctor López
hector.lopez@fje.edu

Seguretat lògica

Control d'accés

Autorització

El mecanisme d'autenticació permet comprovar la identificació d'un usuari perquè accedeixi al sistema o a un recurs concret. Un cop dins, però, l'usuari només podrà fer determinades accions o accedir als recursos als quals se li ha donat permís.

Per facilitar a l'administrador del sistema la tasca d'**autoritzar l'accés als recursos**, es poden establir diferents criteris d'accés mitjançant l'ús de:

- **Rols**
- **Grups**

Seguretat lògica

Polítiques de contrasenyes

- Les contrasenyes són el **mètode més estès** per impedir accessos no autoritzats.
- Són una eina que és molt **econòmica** i ben utilitzada pot ser molt efectiva.
- El **mal ús** de les contrasenyes és a la llista de les **deu amenaces** més habituals de seguretat.
- Una **política** de contrasenyes és un document que **regula** quines són les normes de creació de les contrasenyes, les normes de protecció de les contrasenyes i la freqüència de renovació d'aquestes.

Seguretat lògica

Polítiques de contrasenyes

Contrasenyes febles

- Menys de 10 caràcters.
- Paraules que apareixen els diccionaris.
- Utilitzar informació personal: noms familiars, dates, codis postals...
- Utilitzar patrons numèrics o alfanumèrics: *qwerty, abcd, 1234...*

Seguretat lògica

Polítiques de contrasenyes

Contrasenyes fortes

- Contenir tant majúscules com minúscules.
- Utilitzar valors alfanumèrics (text i números).
- Més de 10 caràcters.
- No utilitzar paraules de diccionaris ni informació personal.

El problema que hi ha amb les contrasenyes robustes és que sovint són difícils de recordar, amb la qual cosa acaben escrites en un tros de paper sota del teclat.

Seguretat lògica

Sistemes biomètrics

Els sistemes biomètrics verifiquen la identitat d'un usuari mitjançant l'anàlisi d'algun dels seus atributs físics o del seu comportament.

- **Basats en un atribut físic:** basen el seu criteri de decisió en alguna cosa que l'usuari és.)

  → Per exemple un lector d'empremtes dactilars.

- **Basats en el comportament:** basen el seu criteri de decisió en alguna cosa que l'usuari fa.

  → Per exemple una tauleta electrònica sobre la qual l'usuari escriu la seva signatura

Seguretat lògica

Sistemes biomètrics

Característiques:

- Sistemes d'autenticació molt cars.
- S'utilitzen en sistemes de seguretat amb requeriments alts.

Hi ha dos tipus d'errors que poden cometre els sistemes biomètrics:

- **Un fals positiu:** es produeix quan el sistema accepta un impostor que hauria d'haver estat denegat.
- **Un fals negatiu:** es produeix quan el sistema denega l'accés a un usuari que hauria d'estar acceptat.