

# LA IDENTITAT. SEGURETAT A LA XARXA

Autor: Felipe Ojeda Perez

Treball per l'assignatura de Tecnologies de la Informació a Dret

Tutor: Albert Balada

## INDEX:

1. [Identitat e identificació a la xarxa](#)
2. [Seguretat a la xarxa](#)
  - Tipus d'autenticació
    - [Identificació vs Autenticació d'usuaris](#)
    - [Basada en prova de coneixement](#)
    - [Basada en quelcom que es té](#)
    - [Sistemes de autenticació biometria](#)
  - [Xarxes privades virtuals \(VPN's\)](#)
  - [Autoritat de registre](#)
  - [Autoritat de certificació](#)
3. [Delictes informàtics](#)
  - [Altres delictes de difícil tipificació](#)
4. [Referències.](#)

## **IDENTITAT E IDENTIFICACIÓ A LA XARXA**

Definició d'identitat presa de **Institut d'Estudis Catalans**

<http://dlc.iec.cat/results.asp?txtEntrada=identitat&operEntrada=0>

**18-05-2009**

### ***identitat***

**1** 1 f. [LC] Qualitat d'idèntic.

**1** 2 f. [LC] Fet d'ésser una persona o una cosa la mateixa que se suposa o se cerca. Comprovar la identitat d'una persona, d'una firma, d'un objecte robat. No s'ha descobert la identitat de l'assassí.

**2** 1 f. [PS] Propietat de l'individu humà de mantenir constantment la pròpia personalitat.

**2** 2 f. [LC] [AN] [SO] Conjunt de característiques que fan que una persona o una comunitat sigui ella mateixa. La llengua forma part essencial de la identitat d'un poble. Identitat nacional.

**3** 1 f. [MT] En mat., igualtat que és satisfeta qualssevol que siguin els valors que donem als seus símbols literals.

**3** 2 f. [MT] Transformació que aplica tot element a ell mateix.

**4** f. [FL] Igualtat que hi ha entre les diverses realitzacions d'un element lingüístic en una mateixa etapa de la llengua o en les diverses etapes de la seva evolució

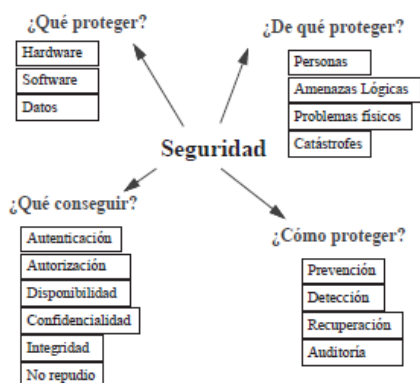
Des del nostre punt de vista serà la segona accepció la que ens interessa, ja que és la que té rellevància a nivell legal.

La identificació d'una persona té a veure amb el fet de comprovar la identitat. De fet en informàtica lo important no es la identificació sinó la autenticació, es dir verificar que la persona que se identifica com tal és realment aquesta.

I la seva importància radica en que l'autenticació permet accedir al sistema informàtic i a les dades que aquest conte, en moltes ocasions modificar aquestes dades i fer un ús fraudulent d'aquesta falsedat de l'autenticació.

## 1. SEGURETAT A LA XARXA

A l'esquema següent es resumeix els diferents criteris vinculats amb la seguretat que cal tindrà en compta:



Com veiem a l'esquema hi ha moltes amenaces a la xarxa, però el gran problema resideix en que, a diferència de la intrusió en documentació en format paper, es algú el que la fa, la intrusió electrònica pot ésser realitzada de manera anònima.

Totes les mesures de seguretat estan basades en intentar evitar-lo. Així l'autenticació de l'usuari es un tret clau en el sistema de seguretat de la xarxa.

Totes les referències que es fan en termes de seguretat son aplicables a la xarxa global: internet, o a xarxes privades: intranet, de forma que els trets de seguretat son semblants.

Es important la protecció davant la intrusió per temes de confidencialitat, integritat i disponibilitat de les dades emmagatzemades.

Aquest termes son molt genèrics, però poden incloure: expedients administratius i jurídics, estats bancaris, llistat de targetes de crèdit-dèbit, expedients mèdics i moltes altres varietats de informes sensibles a la utilització fraudulenta.



La figura següent resumeix la transferència d'informació entre dos sistemes de comunicació, es pot veure com els sistemes informàtics incorporen més complexitat en l'àmbit de la comunicació i de fet faciliten els riscos en seguretat

Tecnologías aplicadas a la seguridad de la información

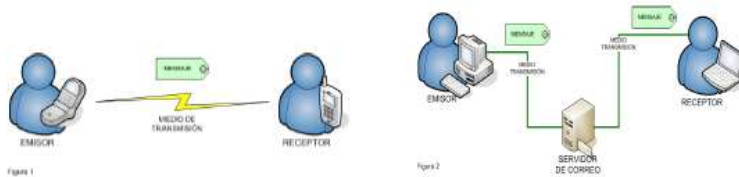
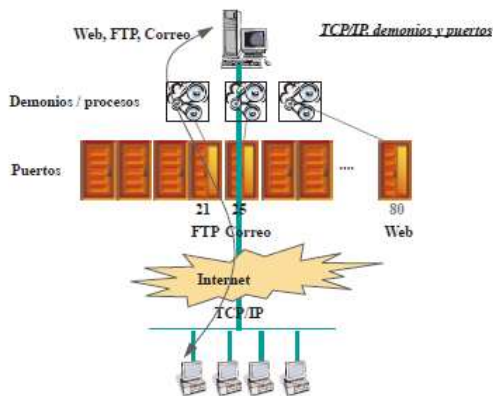


Figura 7.2- Sistemas de comunicación (a) y (b)

Quan anem a la realitat de la societat de la informació actual troben que la complexitat augmenta:



i aquesta complexitat té uns requeriment de seguretat, que en primer lloc afecten no al contingut de la informació sinó al suport físic d'aquest.

Les màquines són susceptibles a atacs i intrusions i normalment tots els sistemes informàtics tenen una primera línia de defensa que es diu firewall (mur de foc).

En els sistemes forts (d'alta seguretat) aquest firewall són de tipus físic, entre les màquines que contenen les dades i l'exterior hi ha interposades altres màquines que conté un software de barrera.

En els sistemes més domèstics el firewall es un programa dintre de nostre ordinador que detecta e impedeix la intrusió. Lamentablement en aquest casos el delinqüent ja esta dintre de la maquina on estan les dades, ja que l'accés s'ha produït per la xarxa, per tant pot intentar forçar el firewall.

En els sistemes robustos això esta dificultat per que ha accedit a una altre maquinari que no te dades.

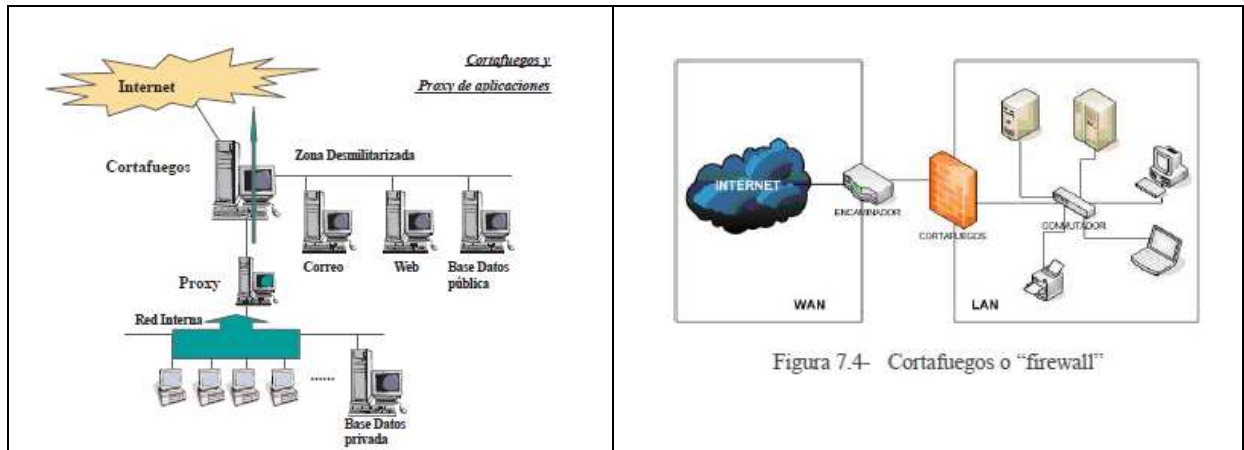
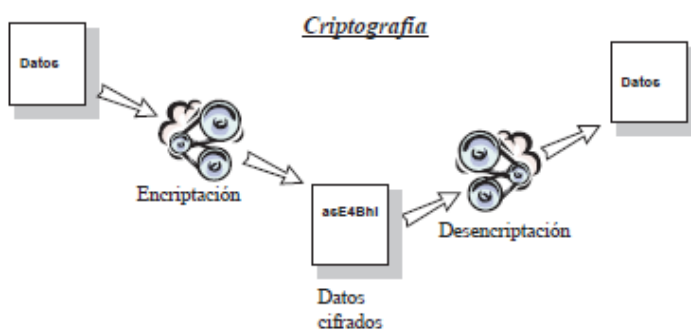


Figura 7.4- Cortafuegos o "firewall"

Aquesta barrera física pot esta vulnerada i davant aquest fet, el següent pas es l'encriptació de les dades, tant en la seva base com al transmetre'ls.

El mecanisme general es mostra al següent gràfic:



Existeixen un munt de sistemes d'enciptació, alguns con un elevat nivell de seguretat, però no es el tema d'aquest treball, per el que si esteu interessat acudiu a la notable bibliografia sobre el tema.

Tenim el maquinari protegit i les dades enciptades, ¿que altres mesures cal tindrè en compta per defensar la seguretat?

Els controls mínims haurien d'ésser:

Monitoratge de les activitat: registre o "logs": inclou la identificació de usuari, l'hora i l'activitat realitzada com mínim.

Trazabilitat: del procés, registre d'activitat i d'accessos

Registre d'accessos: La actual Ley de Protección de Datos (LPD) obliga a registrar tots els accessos.

Possibilitat de bloqueig. Es necessari poder bloquejar l'accés en segons quines condicions: excessiu consum de recursos, fallada de "password " en mes de tres ocasions, baixa de l'usuari, tasques de manteniment, etc.

## Identificació vs Autenticació d'usuaris

Habitualment identifiquem a les persones per l'aspecte físic, forma de parlar, etc son molt complexes per poder, actualment, executar per mitja d'un ordenador.

Així no es proposa identificar l'usuari sinó autenticar que és qui diu ésser.

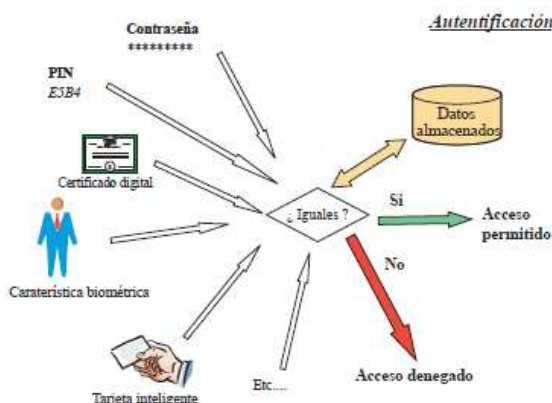
Els mitjans de fer-lo es divideixen en tres categories:

1/ quelcom que sap l'usuari (password, passphrase, PGP)

2/ quelcom que posseeix (tarja, marca digital, etc)

3/ una característica física biomètrica (dactilar, iris, etc)

El gràfic següent resumeix l'autenticació



## TIPUS D'AUTENTIFICACIÓ

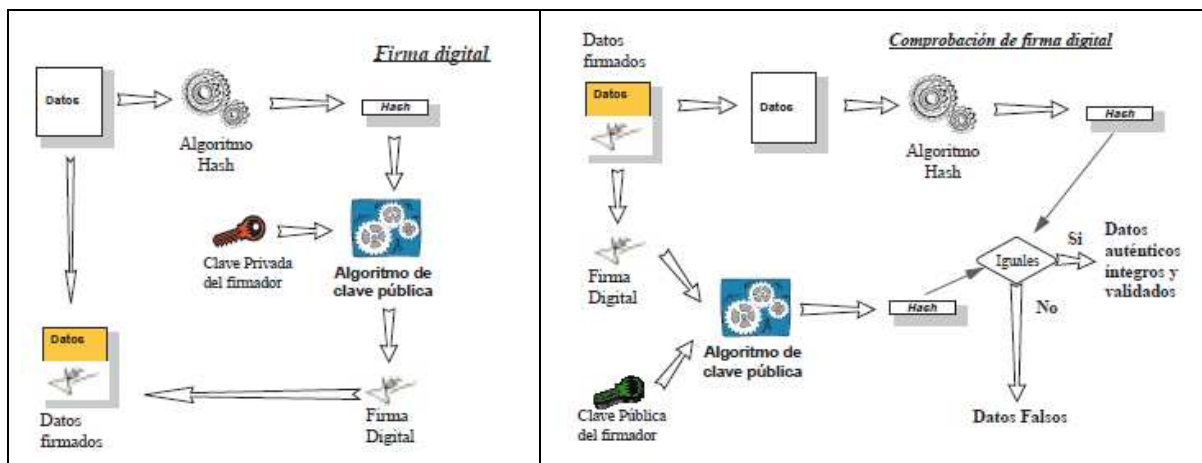
### Basada en prova de coneixement

#### **Password**

Es el sistema més vulnerable, però es el més barat i per tant molt utilitzat en entorn que no precisen alt nivell de seguretat

**Sistemes encriptats de contrasenyes:** son sistemes com els utilitzas en PGP, tant el receptor com l'emisor disposen de claus encriptades i claus públiques relacionades entre ells.

**Signatura digital:** es un sistema més complexe, pel qual una vegada la signatura digital es validada permet la realització de transaccions segures. Es un sistema utilitzat en el marc de les certificacions (veure més endavant)



### Basada en quelcom que es té.

El millor exemple es la **tarja intel·ligent**, la majoria d'aquestes porten o una banda magnètica amb la informació o un xip electrònic. Normalment contenen un certificat digital amb firma electrònica per validar les transaccions.

Un **certificat digital** conté les dades de l'usuari i la seva clau pública (lligada a la privada, aquesta encriptada). Aquesta informació esta avalada per una tercera entitat que garanteix el contingut: l'entitat certificadora. Aquesta valida el contingut signant digitalment tot el certificat, així per validar el contingut només cal comprovar la firma del certificat.



Tipus de certificats i la seva utilitat:

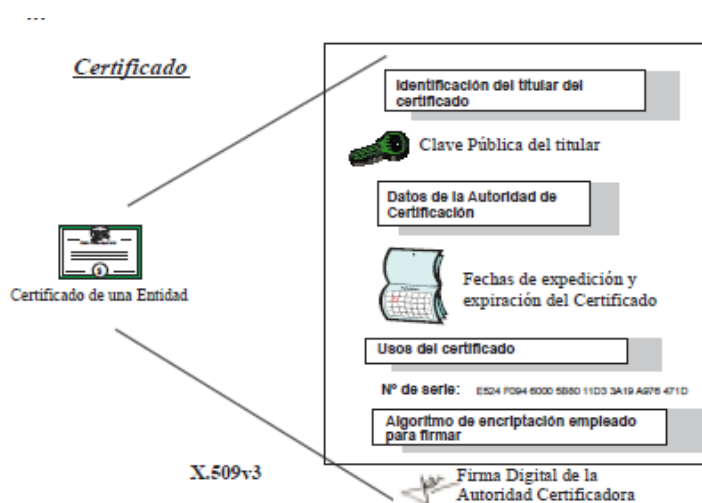
PERSONALS:

- Signatura digital
- xifrat de correu electrònic (S/MIME)
- Signatura de formularis
- SSL
- Solucions de Single-Sign-On (identificació única)

DE SERVIDOR (empreses e institucions)

- SSL
- Time stamp
- VPN's

La figura següent il·lustra el tema del certificat



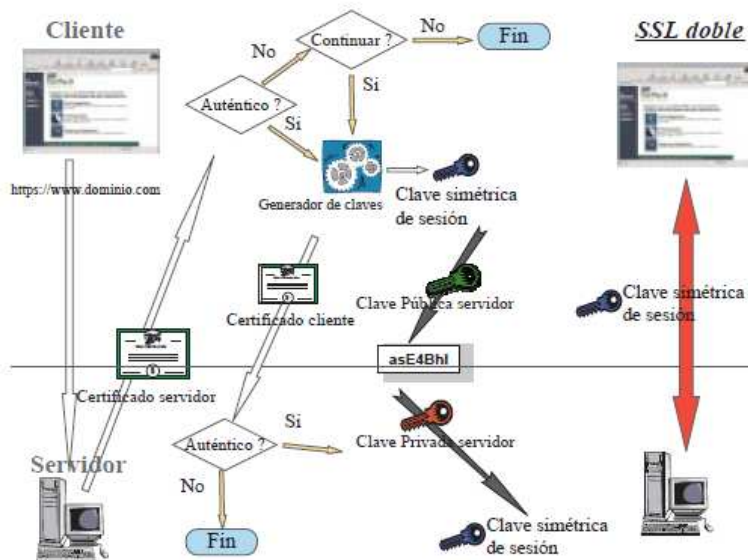
L'existència de certificat obliga a l'existència d'autoritats de certificació: En les referències finals es troba la llista d'aquestes autoritats.

- Autoridad de certificación
  - Firma digital de certificados
  - Firma digital de CRL's
- Firma de código
  - Autenticidad del software

## Comunicació segura amb servidor

**SSL** (Secure Sockets Layer) creat per Netscape, i **TLS** (Transport Layer Security) obert i basat en SSL, aporten una capa de seguretat per garantir l'autenticitat, integritat i confidencialitat en les comunicacions.

SSL es el protocol que utilitzen al connectar amb llocs segurs amb el nostre navegador.



## Smart Cards (Tarjes intel·ligents)

Son un dispositiu de seguretat de mides d'una tarja de crèdit que emmagatzement i procesament segurs d'informació: portan un xip

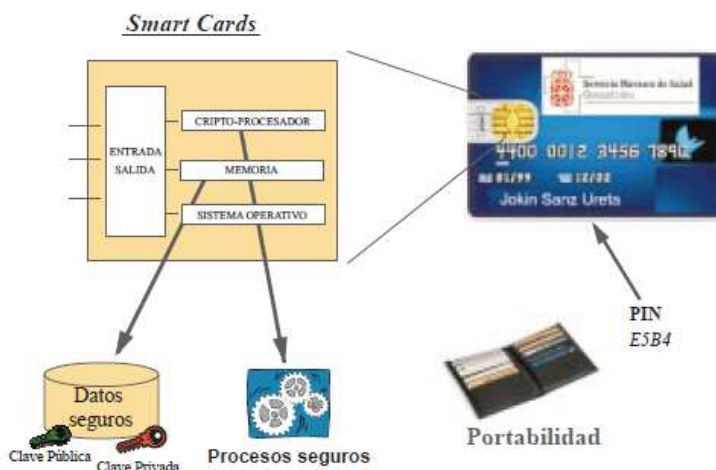
Resistència als atacs per claus privades

Aïllament dels processos d'autenticació, signatura digital e intercanvi de claus

Portabilitat

Doble seguretat: quelcom que té i quelcom que sap (PIN identificatiu)

La funcionalitat es la mateixa que els certificats digitals



## Sistemas de autenticació biometria

Fan us de característiques físiques de l'usuari. A la següent taula es resumeixen les seves característiques:

En la siguiente tabla se muestra una comparativa de los rasgos más generales de los distintos sistemas biométricos:

MÉTODOS ASPECTOS	Ojo – Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta

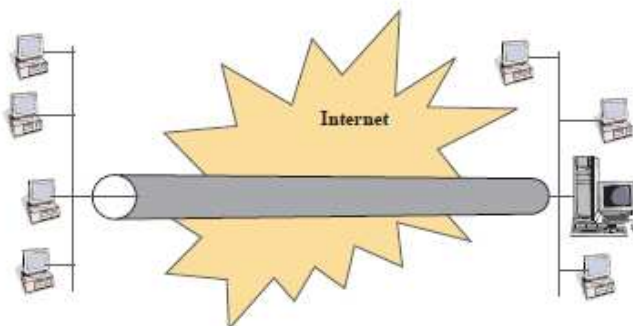
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación/ autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Iritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firma fácil o cambiante	Ruido, resfriados ..
Utilización	Instalaciones nucleares, servicios médicos, penitenciarias	Instalaciones nucleares, servicios médicos, penitenciarias	Policia, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio x nodo	Alto	Alto	Bajo	Medio	Bajo	Bajo

Tabla 7A- Comparativa de métodos biométricos

## Xarxes privades virtuals (VPN's)

Es una tecnologia que permet crea xarxes virtuals protegides:

VPN (Red Privada Virtual)



## **Autoritat de registre**

La *Autoritat de Registre (RA)* es una entitat autoritzada per la *Autoritat de Certificació (CA)* per auxiliar-la en el procés d'assegurar que els usuaris satisfan tots els requisits per l'expedició d'un certificat, es dir, se encarrega de *donar fe* davant la CA de la validesa de les dades que li envia.

Aquestes son les funcions:

–Rebre les sol·licituds de certificació i mantindrà una base de dades. Les sol·licituds poden ser de dos tipus:

1.–De signatura de certificat (*CSR, Certificate Signing Request*). El sol·licitant ha creat, amb un software, la parella de claus privada-pública i, amb les seves dades d'identificació, porta a la RA la clau pública per ser signada.

2.–De creació de certificat complet. El sol·licitant només porta les dades identificatives i rebrà el certificat i la clau privada associada.

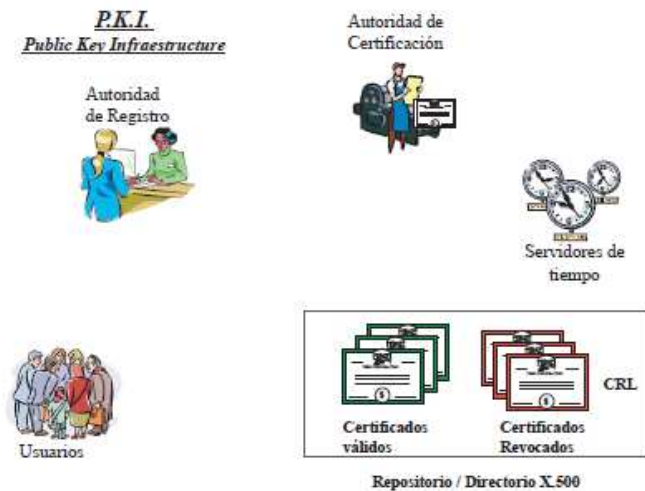
–Rebut de sol·licituds de revocació de certificats prèvies a la expiració d'aquests.

–Sol·licituds de renovació de certificats abans de la seva expiració. La RA ha d'advertir als clients de la necessitat de renovació dels certificats abans de situacions de denegació de servei.

–Decidir la validació o denegació de totes aquestes sol·licituds.

–Mantenir una base de dades amb totes les sol·licituds.

–Generalment la publicació en el repositori corresponent dels certificats i llistes de certificats revocats.



## **Autoritat de certificació**

La *Autoritat de Certificació (CA)* es una entitat de prestigi i confiança que *dona fe* de que una clau pública pertany realment a l'entitat que consta en el certificat.

Funcions:

- Rebre las peticions de la RA i generar els certificats.  
   En funció del tipus de sol·licitud:
  - 1.- el sol·licitant porta la clau pública, amb les dades associades, tan sols signa digitalment amb la seva clau privada.
  - 2.- el sol·licitant porta les dades identificatives, la CA crea la parella de claus i després signa.
  
- Fer a mans els certificats i, si pertoca, les claus privades a la RA.
  
- Generar les *Llistes de Certificats Revocats (CRL)* per que es publiquen en el repositori. En la CRL es troben els números de sèrie dels certificats revocats, signats per la CA per garantir la seva validesa.

## **Entitats de certificació Espanyoles:**

-El proyecto *CERES* (CERTificación ESpañola) de la FNMT (Fábrica Nacional de Moneda y Timbre) ha creat una Entidad Pública de Certificación amb l'objectiu d'assegurar les comunicacions electròniques dels ciutadans amb l'Administració.

-*ACE* (Agencia de Certificación Española), en 1997 amb socis com Telefónica, Sistema 4B, SERMEPA y CECA. Proporciona certificació sota SET y X.509v3.

-*FESTE* (Fundación para el Estudio de la Seguridad en las Telecomunicaciones) integrat pels Notaris, corredors de comerç i la Universidad de Zaragoza. Actua com servei de certificació.

-*CAMERFIRMA* esta basat en las Cambres de Comerç de tota Europa. Proporciona certificació sota X.509v3.

Des de fa uns anys existeixen autoritat de certificació autonòmiques (veure en referències)

## **Internacionals:**

- VeriSign
- SecureNet
- Entrust

a Catalunya dispossem de CATCERT, agencia pròpia de certificació:



<http://www.catcert.cat/web/cat/index.jsp>

Es l'agència catalana de certificació, ofereix els següents serveis:

## **CERTIFICATS DIGITALS**

- [Certificat Personal d'Identificació i Signatura Reconeguda + Certificat Personal de Xifrat \(CPISR-1 + CPX-1\)](#)
- [Certificat Personal d'Identificació i Signatura Reconeguda amb Càrrec \(CPISRC-1\) + Certificat Personal de Xifrat amb Càrrec \(CPXC-1\)](#)
- [Certificat d'Entitat de signatura reconeguda + Certificat d'Entitat de Xifrat \(CESR+CEX-1\)](#)
- [Certificat de dispositiu servidor \(CDS\)](#)

- [Certificat de dispositiu de servidor de controlador de domini segur \(CSDSC\)](#)
- [Certificat de dispositiu programari \(CDP\)](#)
- [Certificat de dispositiu d'aplicació \(CDA\)](#)

En part, hem presentat algunes de les característiques tècniques que influeixen en els temes de seguretat referida a l'autenticació. A les pàgines següents intentarem classificar els possibles delictes relacionats amb aquest tema.

### 3. DELICTES INFORMÀTICS:

Delictes informàtics son aquest delictes contemplats en el codi penal com tal, i que per la seva realització s'utilitza elements informàtics. Ex: estafa, contra la propietat intel·lectual e industrial, etc.

Abans, amb el CP 1975 el redactat en el tema de l'estafa

*"Art. 528. El que defraudare a otro en la sustancia, cantidad o calidad de las cosas que le entregare en virtud de un delito obligatorio será castigado [...]."*

*Art. 529. El que defraudare a otro usando nombre fingido, atribuyéndose poder, influencia o cualidades supuestas, aparentando bienes, crédito saldo en cuenta corriente, comisión, empresa o negociaciones imaginarias o valiéndose de cualquier otro engaño semejante [...]. Cometen estafa los que con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndole a realizar un acto a disposición en perjuicio propio o ajeno. También se consideran reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación [...]."*

Molt delictes practicats amb eines informàtiques varen ésser tipificats com apropiació indeguda.

El nou Codi Penal, de 23 de noviembre de 1995, inclou de manera específica el tema informàtic:

*Artículo 248. También se consideran reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. La misma pena se aplicará a los que fabriquen, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de estafas previstas en este artículo.*

*Malgrat tot, no estan tots clarament tipificats, per exemple l'apologia de terrorisme per mitjans de pàgines web. Ni l'utilització d'aquestes en la propagació de doctrines violentes.*

Tipus de delictes informàtics contemplats:

Amenaces. Tal i com es contemplen a la legislació, malgrat que ho siguin en format electrònic, no de paraula o per escrit.



Delictes d'**exhibicionisme i provocació sexual**.

Delictes relatius a **prostitució i corrupció de menors**.

**Delictes contra la intimitat**, el dret a la pròpia imatge i la inviolabilitat de domicili: El descobriment i revelació de secrets, p.e. La intercepció de correu vendria assimilada a la violació de correspondència, sempre que no existeixi consentiment i existeix intenció de desvelar secrets o vulnerar la intimitat de un tercer. També la usurpació i cessió de dades reservades de caràcter personal.

**Delictes contra l'honor**: Calumnies e injúries, en especial si es realitzen amb publicitat

Les **estafes**. Tal i com es contemplen en termes generals en la legislació i jurisprudència

Les **defraudacions de fluid elèctric**. Inclou la defraudació en telecomunicacions sempre i quan s'utilitza un mecanisme o alterant maliciosament les indicacions o s'utilitzin mitjans clandestins. També les manipulacions de telèfons mòbils, etc

Els **danys**. Destaca de l'ampliació de la definició existent, incloent un apartat per els immaterials "La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos". Aixó intenta protegir la propietat intel·lectual en soportes informàtics: ex. Pàgines web.

Delictes relatius a la **propietat intel·lectual** ([Cómo proteger las creaciones y proyectos que se desarrollan en mi empresa](#)).

Els delictes relatius a la **propietat industrial** ([Test de propiedad industrial](#)).

**Delictes relatius al mercat i als consumidors.** publicitat enganyosa publicada o difosa per Internet, sempre i quan es facin alegacions falses o manifesten característiques incertes que puguin originar un perjudici greu i manifest als consumidors. ([¿Son mis invenciones patentables?](#))

### **Altres delictes de difícil tipificació:**

El spam, el scanneig de ports, comerç electrònic, etc. que no tenen cabuda en el Código Penal, si la tenen en el marc de les lleis de protecció de dades personals (Ley Orgánica de Protección de Datos Personales); quan es tracta de qüestions de societat de la informació o temes de correus electrònics també en la llei específica (Ley de Servicios de la Sociedad de la Información y Comercio Electrónico).

Les denúncies cal presentar-les davant la Agencia Española de Protección de Datos o en el marc de Catalunya en la pròpia agència (veure més endavant). Aquestes denúncies tenen caire gratuït. Si el tema té relació amb telecomunicacions, correu, spam, etc: la denúncia cal interposar-la davant la Secretaria de Estado de Telecomunicaciones y Sociedad de la Información, adscrita al Ministerio de Industria, Turismo y Comercio”

<http://www.diariojuridico.com/asides/datos-curiosos-de-delitos-en-internet.html>

## REFERÈNCIES LEGALS:

Legislació comunitària sobre protecció de dades:

### Consell d'Europa

- [Convenció per a la salvaguarda dels drets humans i de les llibertats fonamentals](#)
- [Convenció per a la protecció de les persones pel que fa al tractament automatitzat de dades de caràcter personal, fet a Estrasburg el 28 de gener de 1981](#)

### Unió Europea

- [ [CAT](#) | [ESP](#) | [ENG](#) | [FR](#) ] Carta del drets fonamentals de la Unió Europea (arts. 7 i 8)
- [ [CAT](#) | [ESP](#) | [ENG](#) | [FR](#) ] Directiva 95/46/CE, del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades
- [ [CAT](#) | [ESP](#) | [ENG](#) | [FR](#) ] Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques
- [ [CAT](#) | [ESP](#) | [ENG](#) | [FR](#) ] Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de març de 2006, sobre la conservació de dades generades o tractades en relació amb la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions i per la qual es modifica la Directiva 2002/58/CE
- [ [ESP](#) | [ENG](#) | [FR](#) ] Decisió Marc 2008/977/JAI del Consell, de 27 de novembre de 2008, relativa a la protecció de dades personals tractades en el marc de la cooperació policial i judicial en la matèria penal

### [Protección de datos por las instituciones y organismos de la Comunidad](#)

El Reglamento está destinado a garantizar la protección de los datos personales en el marco de las instituciones y organismos de la Unión Europea (tags: reglamento protección organismos instituciones de datos)

### [Protección de los datos personales. Sociedad Información](#)

La presente Directiva se aplica a los datos tratados por medios automatizados, así como a los datos contenidos en un fichero

no automatizado o que vayan a figurar en él. (tags: protección datos)

#### [Fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad](#)

Fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (tags: tecnologías protección la intimidad derecho de datos)

#### [Seguridad de los sistemas de información](#)

(tags: sistemas seguridad protección información de datos)

#### [Protección de datos en el sector de las comunicaciones electrónicas](#)

protección de datos en comunicaciones (tags: protección electronicas datos comunicaciones)

#### [Seguimiento de los procedimientos interinstitucionales. Prelex](#)

Prelex (tags: prelex legislación)

#### [Legislación vigente](#)

Espacio de libertad, seguridad y justicia (tags: seguridad libertad legislación justicia)

#### [Tratado constitutivo 61-69](#)

(tags: union seguridad libertad justicia europea)

#### [Artículos 20-30 del Tratado de la Unión](#)

Artículos 20-30 del Tratado de la Unión (tags: union tratado seguridad libertad justicia)

#### [Libertad, seguridad y justicia para todos](#)

Justicia y Asuntos de interior de la Unión Europea (tags: union seguridad libertad justicia europea)

#### [Questions and Answers](#)

Preguntas y respuestas generales sobre protección de datos y la Oficina Europea (tags: union respuestas protección preguntas europea edps datos)

#### [Legislation in data protection](#)

Legislación de la Unión europea en materia de protección de datos (tags: union protección legislación europea datos)

#### [Supervisor Europeo de Protección de Datos](#)

La portada es en castellano, los textos posteriores en inglés o francés. (tags: protección datos)

#### [Justicia. Unión Europea](#)

Página de Justicia, Libertad y Seguridad (tags: seguridad libertad justicia)

#### [Portal Europa](#)

Portal de entrada: toda la información sobre la Unión Europea organizado temáticamente. (tags: union temas portal europeos europea)



<https://www.agpd.es/portalweb/index-ides-idphp.php>

## Estatal

↓ [Constitución Española de 1978.](#)

---

Ley:

↓ [Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.](#)

---

↓ [Versión en inglés de la Ley Orgánica 15/1999](#)

---

Real Decreto:

↓ [Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.](#)

---

↓ (\*) [Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados.](#)

---

↓ (\*) [Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.](#)

---

↓ [Versión en inglés del Real Decreto 994/1999](#)

---

↓ [Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 428/1993, de 26 de marzo.](#)

---

[↓Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos.](#)

---

[↓\(\\*\) Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica.](#)

---

[↓Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos](#)

(\*) Normas derogadas a la entrada en vigor del Real Decreto 1720/2007, de 21 de diciembre.

Normas de carácter reglamentario:

1.- Resoluciones:

[↓Resolución de 8 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se corrigen errores en las Resoluciones de 12 de julio de 2006, por las que se crea el Registro Telemático y se aprueban los formularios electrónicos para inscribir los ficheros en el Registro General de Protección de Datos.](#)

---

[↓Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos.](#)

---

[↓Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos.](#)

---

[↓Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático.](#)

---

[↓Resolución de 22 de junio de 2001, de la Subsecretaría de Justicia, que concreta el plazo para la implantación de medidas de seguridad de nivel alto.](#)

---

[↓Resolución de 30 de mayo de 2000, de la APD, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático, para la inscripción de los ficheros.](#)

---

## 2.- Instrucciones:

[↓Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.](#)

---

- [Descarga de Modelos de Videovigilancia](#)

[↓Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones.](#)

---

[↓Instrucción 2/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.](#)

---

[↓Instrucción 1/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.](#)

---

[↓Instrucción 2/1995, de 4 de mayo, de la APD, sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal.](#)

## CATALUNYA



Agència Catalana de Protecció de Dades

Agencia Catalana de Protecció de Dades.

[↓Ley 5/2002 \(Comunidad Autónoma de Cataluña\), de 19 de abril, de la Agencia Catalana de Protección de Datos.](#)

## Normativa reguladora de l'Agència

- [ [CAT](#) | [ESP](#) ] Estatut d'autonomia de Catalunya (art. 4.1, 15, 20, 23, 27, 28, 30, 31, 76, 78, 156, 182.3) (DOGC núm. 4680, de 20.07.06)
- [ [CAT](#) | [ESP](#) ] Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades (DOGC núm. 3625, de 29.04.2002)

- [ [CAT](#) | [ESP](#) ] Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades (DOGC núm. 3835, de 04.03.2003)