Responsabilitat i aspectes legals de la protecció de dades personals en els sistemes d'informació sanitaris

Natalia Almudevar Arnal
Anna García Martínez

PID_00167312

UOC
Universitat Oberta de Catalunya

Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca

Índex

1. Règim jurídic de la protecció de dades 5
1.1. La protecció de dades en l'àmbit sanitari 5
1.2. Aspectes bàsics de la protecció de dades 6
1.2.1. Origen i evolució legislativa 6
1.2.2. La protecció de dades. Definició 7
1.2.3. Àmbit d'aplicació 7
1.3. LOPD: principals obligacions de la normativa sobre protecció de dades 8
1.3.1. Notificació de la creació, modificació o supressió de fitxers 8
1.3.2. Principis de la protecció de dades 11
1.3.3. Drets dels afectats 16
1.4. Reglament de mesures de seguretat 18
1.4.1. Objecte i àmbit d'aplicació 18
1.4.2. Nivells de seguretat 19
1.4.3. Mesures de seguretat 19
1.5. Règim sancionador 21
1.5.1. Autoritats de control 21
1.5.2. Infraccions i sancions 22

2. Introducció als elements tècnics de models de seguretat 25
2.1. Fonaments de seguretat tècnica 25
2.1.1. Nivells de seguretat 28
2.2. Signatura electrònica i criptografia 32
2.2.1. Identificació i autenticació 32
2.2.2. Nocions bàsiques de criptografia 33
2.2.3. Validesa legal i regulació de la signatura electrònica 34
2.3. Pla director de seguretat 35

3. Annexos 39
3.1. Legislació 39
3.2. Una altra documentació d'interès 40
3.3. Recursos a Internet 41

1. Règim jurídic de la protecció de dades

1.1. La protecció de dades en l'àmbit sanitari

Les dades tractades en l'àmbit sanitari són necessàries per a prestar adequadament l'atenció sanitària a la qual els ciutadans tenen dret; si bé, més enllà d'aquesta esfera de prestació sanitària, existeix l'àmbit de la intimitat de les persones, que requereix que els professionals sanitaris, i també els gerents dels centres sanitaris, observin els principis de la normativa sobre protecció de dades personals i donin compliment a les obligacions que recull.

La normativa sobre protecció de dades personals i, en particular, la LOPD (Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal), té com a finalitat:

> "[...] garantir i protegir, pel que fa al tractament de dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i intimitat personal i familiar".

Per tant, i atenent a la definició que aquesta norma estableix de *fitxer*, "[...] tot conjunt organitzat de dades de caràcter personal, qualsevol que sigui la forma o modalitat de la seva creació, l'emmagatzematge, l'organització i l'accés", queda patent que tant la gestió de la història clínica, com qualsevol altre tractament de dades personals fet pels centres sanitaris queden subjectes a les obligacions d'aquesta normativa.

> La LOPD qualifica les dades relatives a la salut dels ciutadans com a dades especialment protegides, i estableix un règim especialment rigorós per a l'obtenció, el tractament, la custòdia i possibles comunicacions.

Amb l'aprovació de la Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica i, a Catalunya, de la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent a la salut i l'autonomia del pacient i la documentació clínica, es regula per primera vegada d'una manera específica la història clínica i la protecció de dades mèdiques.

1.2. Aspectes bàsics de la protecció de dades

1.2.1. Origen i evolució legislativa

La normativa sobre protecció de dades personals sorgeix com a conseqüència de la preocupació del legislador davant els riscos associats al desenvolupament de les noves tecnologies. El desenvolupament de grans computadores es considera com una nova amenaça potencial ateses les possibilitats que ofereixen per als tractaments massius d'informació.

Això fa que el legislador consideri necessari regular aquests aspectes amb la finalitat de protegir la intimitat dels ciutadans, la qual cosa es duu a terme mitjançant el mandat al legislador recollit en la Constitució de 1978, que estableix en l'article 18.4 que "la llei limitarà l'ús de la informàtica per a garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets".

No és fins al 1992 que aquest mandat és desenvolupat amb l'aprovació de la LORTAD (Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de les dades de caràcter personal), la qual, i atenent a l'establert en l'articulat, tenia per objecte:

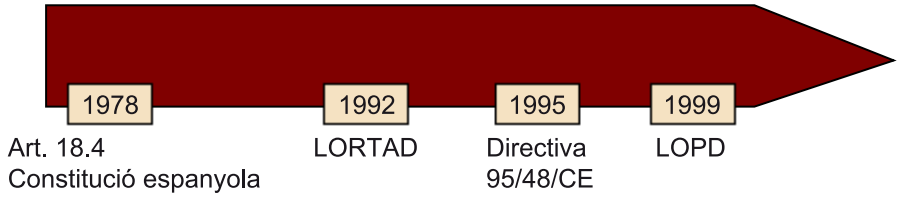
> "[...]limitar l'ús de la informàtica i altres tècniques i mitjans de tractament automatitzat de les dades de caràcter personal per a garantir l'honor, la intimitat personal i familiar de les persones físiques i el ple exercici dels seus drets".

Hem de destacar que, atès que la preocupació era el desenvolupament progressiu de les tècniques de recol·lecció i emmagatzematge de dades i d'accés a les dades, l'àmbit d'aplicació de la LORTAD es limitava a les dades de caràcter personal que figuressin en fitxers automatitzats.

L'aprovació, el 1995, de la Directiva 95/46/CE estableix un marc comú per a tots els països membres de la Unió Europea, ampliant l'àmbit d'aplicació:

> "Les disposicions d'aquesta directiva s'aplicaran al tractament totalment o parcialment automatitzat de dades personals, i també al tractament no automatitzat de dades personals contingudes o destinades a ser incloses en un fitxer."
>
> 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.

Finalment, el desembre de 1999, es publica la LOPD, que té com a novetat principal ampliar l'àmbit d'aplicació a tot tipus de fitxers, independentment del suport en el qual siguin tractats. Així mateix, s'adequa a l'establert en la directiva. En l'actualitat, és la norma bàsica vigent en matèria de protecció de dades personals.



Principals fites legislatives en matèria de protecció de dades personals

1.2.2. La protecció de dades. Definició

El dret a la protecció de dades és un dret fonamental de totes les persones, que es tradueix en la potestat de control sobre l'ús que se'n fa de les dades personals.

Després de l'aprovació de la LOPD, la Sentència 292/2000 del Tribunal Constitucional reconeix el dret a la protecció de dades com un dret fonamental independent del dret a l'honor, intimitat i imatge, i, d'aquesta manera, dota la protecció de dades de caràcter personal d'identitat pròpia i independent de qualsevol altre dret fonamental.

Per tant, tota organització pública o privada que tracti dades personals està obligada a complir els requeriments establerts en la LOPD, normativa de desenvolupament i normativa sectorial aplicable.

Com a premissa, hauríem d'identificar què s'entén per *dada personal*. Atenent a la definició establerta per la LOPD, una *dada personal* és "qualsevol informació concernent a persones físiques identificades o identificables". Això representa que en el moment en què es reculli o es tracti informació, com, per exemple, nom i cognoms, DNI, adreça de correu electrònic, nombre d'història clínica, imatge, qualsevol codi d'identificació personal, etc., serem davant un fitxer objecte de la normativa.

1.2.3. Àmbit d'aplicació

Des de l'aprovació de la LOPD, la normativa vigent s'aplica a les dades de caràcter personal registrades en qualsevol suport que les faci susceptibles de tractament, i també al seu ús posterior:

- Suport informàtic: aplicacions, bases de dades, etc.

- Suporti paper: fitxers manuals organitzats que recullin tota la informació clínica d'un procés assistencial a un pacient, l'expedient d'un treballador, etc.

La normativa s'aplica tant als fitxers públics (titularitat de l'Administració), com a fitxers privats (titularitat d'empreses) sempre que continguin dades personals.

La normativa no s'aplica a:

- Fitxers que hagin estat sotmesos a un procediment de dissociació; és a dir, que no sigui possible associar la informació a una persona física identificada o identificable.

- Fitxers mantinguts per persones físiques en l'exercici de les seves activitats personals o domèstiques.

- Fitxers relatius a matèries classificades.

- Fitxers relatius a terrorisme o delinqüència organitzada.

Hi ha una sèrie de supòsits en els quals els fitxers s'hauran de regir per les seves disposicions específiques i pel previst especialment en la LOPD, com és el cas dels fitxers estadístics, entenent per *fitxer estadístic* el que serveixi a finalitats exclusivament estadístiques i estigui emparat per la legislació estatal o autonòmica sobre la funció estadística pública. Així mateix, estan subjectes a règim específic:

- els fitxers regulats per la legislació de règim electoral,
- els fitxers de les forces armades,
- el Registre Civil i Registre de Penats i Rebels,
- càmeres de vídeo de cossos i forces de seguretat.

No són objecte de la normativa les dades relatives a les persones jurídiques.

1.3. LOPD: principals obligacions de la normativa sobre protecció de dades

1.3.1. Notificació de la creació, modificació o supressió de fitxers

Una de les principals obligacions establertes per la normativa és la de notificar a l'autoritat de control corresponent la creació de fitxers que continguin dades personals. En cas que ja existeixin, se n'haurà de notificar a l'autoritat de control corresponent la modificació o supressió.

Entitats privades

L'article 25 de la LOPD estableix:

> "Es poden crear fitxers de titularitat privada que continguin dades de caràcter personal quan resulti necessari per a l'assoliment de l'activitat o objecte legítim de la persona, empresa o entitat titular i es respectin les garanties que aquesta llei estableix per a la protecció de les persones."

A més, l'article 26.1 LOPD estableix:

> "Qualsevol persona o entitat que procedeixi a la creació de fitxers de dades de caràcter personal ho haurà de notificar prèviament a l'Agència Espanyola de Protecció de Dades".

Prèviament a la notificació de fitxers tractats, s'han d'identificar els tractaments de dades fets. Per a això, és necessari mantenir entrevistes amb les àrees que tracten les dades personals amb la finalitat d'identificar-ne l'origen, tipologia, finalitats del tractament, tractaments efectuats, nivell de seguretat que cal aplicar, cessions o comunicacions de dades i transferències internacionals de dades.

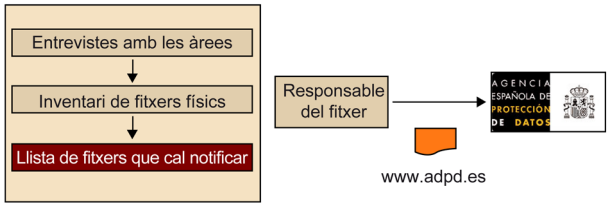
Una vegada obtinguda la relació de fitxers tractats per les diferents àrees, s'han d'agrupar creant fitxers lògics per a notificar-ne a l'Agència Espanyola de Protecció de Dades la creació o el tractament.

Els fitxers lògics

Els fitxers lògics agrupen determinats fitxers físics (o de nivell més baix), que compleixen uns requisits determinats que permeten la seva agrupació per a poder notificar a l'autoritat corresponent dades com la seva finalitat, les característiques bàsiques del seu tractament i el seu nivell de seguretat.

Un fitxer lògic de personal pot contenir diferents fitxers, com, per exemple, un arxiu Excel per a gestionar la formació, o una base de dades que contingui els torns dels treballadors.

Requisit imprescindible per a la creació de fitxers nous de dades de caràcter personal és la inscripció prèvia en el Registre de l'Agència Espanyola de Protecció de Dades.



Identificació i notificació de fitxers en entitats privades

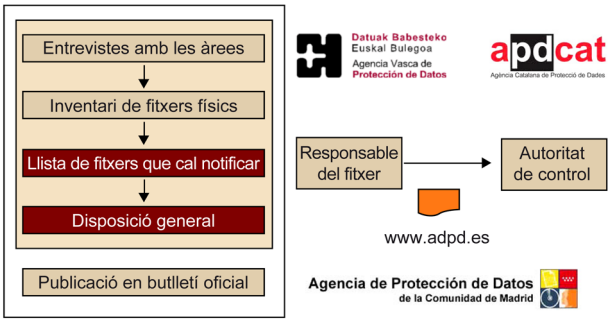
Entitats públiques

Tal com recull l'article 20.1 de la LOPD:

"La creació, modificació o supressió de fitxers de les administracions públiques només es poden fer per mitjà de disposició general publicada en el Butlletí Oficial de l'Estat o diari oficial corresponent".

Així, per a la creació d'un fitxer de titularitat pública, l'organisme competent ha d'aprovar una disposició, que haurà de ser publicada en el butlletí oficial corresponent. Una vegada aprovada la disposició, cal notificar la creació del fitxer a l'autoritat de control competent.

Una vegada més, és necessari fer el procés previ d'identificació dels fitxers físics tractats per l'organització amb la finalitat d'agrupar-los en fitxers lògics. Aquest procés d'inventari de la informació permet mantenir actualitzades les notificacions a l'autoritat de control competent (modificacions i supressions).



Identificació i notificació de fitxers en entitats públiques

Fitxers tipus en una organització sanitària

A manera d'exemple, s'ofereix una compilació dels possibles fitxers que un hospital tipus ha de notificar a l'autoritat de control corresponent:

Fitxer que cal notificar (fitxer lògic)	Fitxers físics
Pacients	Històries clíniques Laboratori Urgències Registre de consentiment informat Resultats de proves diagnòstiques Sala d'operacions ...
Nòmines	Gestió de nòmines
Personal	Formació Control de torns Gestió de beneficis socials Peticions i sol·licituds del personal ...
Administració i comptabilitat	Gestió de compres Gestió de proveïdors Facturació Comandes ...
Seguretat	Control d'accés Videovigilància ...

1.3.2. Principis de la protecció de dades

Tot responsable de fitxer ha d'establir els mecanismes o els processos interns de la seva organització de manera que es compleixin els principis de la protecció de dades recollits en el títol II de la LOPD i de què tractarem seguidament.

Qualitat de les dades

La qualitat de les dades s'aborda en l'article 4 de la LOPD i és un pilar fonamental d'una bona gestió de la informació, i és especialment important en els sistemes d'informació sanitaris.

El principi de la qualitat de les dades es concreta és els aspectes següents:

- Les dades personals s'han d'adequar a la finalitat per la qual van ser recollides; és a dir, les dades només es poden recollir per al seu tractament i només es poden sotmetre a aquest tractament quan siguin adequades, pertinents i no excessives amb relació a l'àmbit i a les finalitats determinades, explícites i legítimes per les quals s'hagin obtingut.

- Les dades personals no es poden usar per a finalitats incompatibles amb aquelles per les quals haguessin estat recollides.

- Les dades hauran de ser exactes i posades al dia (actualitzades). Això no significa que les organitzacions hagin de mantenir exactes les dades quan no tinguin mitjans per a conèixer-ne l'exactitud; però, si tenen coneixement de la inexactitud d'una dada, l'han d'actualitzar.

- Les dades han de ser cancel·lades quan hagin deixat de ser necessàries per a la finalitat per la qual van ser recollides o registrades; és a dir, no s'han de mantenir indefinidament sense justificació, tret que alguna obligació legal estableixi la necessitat de conservar les dades una vegada conclosa la finalitat que en va motivar la recollida o, si escau, en les relacions contractuals entre la persona o entitat responsable del tractament i la persona interessada. L'organització pot conservar les dades mitjançant el seu bloqueig o previ procés de dissociació.

- Les dades han d'haver estat recollides d'una manera lícita.

Dret d'informació en la recollida de dades

L'article 5.1 de la LOPD estableix l'obligació prèvia d'informar el titular de les dades en el moment de recollir-les, de manera que la persona pugui o no facilitar les seves dades amb ple coneixement del tractament que rebran.

"Els interessats als quals se sol·liciti dades personals hauran de ser prèviament informats d'una manera expressa, precisa i inequívoca:

a) De l'existència d'un fitxer o tractament de dades de caràcter personal, de la finalitat de la seva recollida i dels destinataris de la informació.

b) Del caràcter obligatori o facultatiu de la seva resposta a les preguntes que els siguin plantejades.

c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.

d) De la possibilitat d'exercitar els drets d'accés, rectificació, cancel·lació i oposició.

i) De la identitat i adreça del responsable del tractament o, si escau, del seu representant."

Pel que fa a les dades recollides mitjançant qüestionaris, formularis o altres impresos (en format paper o electrònic), els punts anteriors hi hauran de figurar d'una manera clarament llegible i no serà necessari informar del contingut dels apartats b), c) i d) si es dedueix clarament de la naturalesa de les dades personals que se sol·liciten o de les circumstàncies en què es recullen.

Pel que fa a les **dades recollides de terceres persones**, és a dir, principalment, als supòsits de cessions de dades entre empreses o entre administracions públiques, la LOPD estableix en l'article 5.4, que:

"Quan les dades de caràcter personal no hagin estat recollides de la persona interessada, aquesta haurà de ser informada d'una manera expressa, precisa i inequívoca, pel responsable del fitxer o el seu representant, dins dels tres mesos següents al moment del registre de les dades, tret que ja hagués estat informada amb anterioritat, del contingut del tractament, de la procedència de les dades, i també del previst en les lletres a), d) i e) de l'apartat 1 d'aquest article".

Per això, en el cas d'obtenir dades que no hagin estat directament recollides dels interessats, cal assegurar que l'organització que les facilita hagi complert el deure d'informació; en cas contrari, s'haurà de comunicar a la persona interessada:

- La procedència de les dades.
- El titular del fitxer.
- Les finalitats del tractament.
- El caràcter obligatori/facultatiu de les respostes.
- Els drets que té i la seva possibilitat d'exercici.
- L'adreça i, si escau, les condicions per a exercitar aquests drets.

Les clàusules d'informació han de detallar les finalitats amb les quals es recull la informació.

Model de clàusula d'informació

En compliment de l'establert per la normativa sobre protecció de dades personals, els informem que les seves dades seran incorporades a un fitxer titularitat de [NOM DE L'ORGANITZACIÓ], amb la finalitat de [INDICAR FINALITAT]. Les seves dades seran comunicades a [INDICAR DESTINATARIS] amb la finalitat de [INDICAR FINALITAT]. Pot exercitar els seus drets d'accés, rectificació, cancel·lació i oposició dirigint-se a: [NOM I ADREÇA DE L'ORGANITZACIÓ].

L'article 5.5 LOPD estableix una sèrie d'excepcions **a l'obligació d'informar** quan les dades no procedeixin de la persona interessada:

> "No és aplicable el disposat en l'apartat anterior, quan expressament una llei ho prevegi, quan el tractament tingui finalitats històriques, estadístiques o científiques, o quan la informació a la persona interessada resulti impossible o exigeixi esforços desproporcionats, a criteri de l'Agència de Protecció de Dades o de l'organisme autonòmic equivalent, en consideració al nombre d'interessats, a l'antiguitat de les dades i a les possibles mesures compensatòries."

Consentiment de la persona afectada

El consentiment és la manifestació de voluntat, lliure, inequívoca, específica i informada, per la qual la persona interessada consent el tractament de les seves dades personals.

L'article 6.1 LOPD diu:

> "El tractament de les dades de caràcter personal requereix el consentiment inequívoc de la persona afectada, tret que la llei disposi una altra cosa."

L'obtenció del consentiment se sol fer a l'hora de la recollida de les dades mitjançant la clàusula d'informació, atès que es considera que a partir d'aquesta informació la persona afectada és conscient i pren coneixement de l'existència del tractament que se'n farà, les finalitats i els drets que tingui.

La llei disposa, per a determinades categories de dades, un tipus especial de consentiment. En aquest grup s'inclouen les **dades de salut**, que, com ja s'ha indicat, gaudeixen d'un règim especialment rigorós, que requereix el consentiment exprés per al seu tractament. Concretament, l'article 7.3 LOPD diu:

> "Les dades de caràcter personal que facin referència a l'origen racial, a la salut i a la vida sexual només poden ser recollides, tractades i cedides quan, per raons d'interès general, així ho disposi una llei o la persona afectada ho consenti expressament."

En cas de tractament d'aquesta tipologia de dades, serà necessari que l'organització acrediti que ha obtingut el consentiment de la persona interessada amb totes les garanties establertes per la llei; és a dir, que el consentiment sigui lliure, inequívoc, específic, informat i prestat per escrit i d'una manera expressa.

Amb la finalitat de conciliar les obligacions de la normativa sobre protecció de dades personals amb altres béns jurídics que igualment mereixen protecció, la LOPD estableix en l'article 6.2 una sèrie d'excepcions **al consentiment**. D'acord amb aquest article, no és necessari el consentiment previ de la persona afectada per al tractament de les seves dades personals en els casos següents:

- Dades recollides per a l'exercici de les funcions pròpies de les administracions públiques.
- Dades relatives a les parts d'un contracte o precontracte d'una relació negocial, laboral o administrativa.

- Quan el tractament de dades sigui necessari per a protegir un interès vital de la persona interessada.
- Dades provinents de fonts accessibles al públic.

Pel que fa a les dades relatives a l'origen racial, a la salut i a la vida sexual, encara que per norma requereixen el consentiment exprés de la persona interessada, la norma també estableix una sèrie d'excepcions:

- Quan el tractament de dades sigui necessari per a la prevenció o diagnòstics mèdics, la prestació d'assistència sanitària o tractaments mèdics o la gestió de serveis sanitaris.

- Sempre que el tractament de dades el faci un professional sanitari subjecte al secret professional o una altra persona subjecta així mateix a una obligació equivalent de secret.

- Quan el tractament de dades sigui necessari per a salvaguardar l'interès vital d'una persona afectada o d'una altra persona, en cas que l'afectat estigui físicament o jurídicament incapacitat per a atorgar el consentiment.

Comunicació de dades

Es considera *cessió de dades* qualsevol revelació de dades feta per persona diferent de la interessada, entenent per *cessió* qualsevol forma d'accés d'un tercer a la informació (lliurament, comunicació, consulta, transferència...).

Seguint l'establert en l'article 11 LOPD, en tota cessió de dades han de concórrer els requisits següents:

- Que només és possible la cessió de les dades per al compliment de finalitats directament relacionades amb les funcions de cedent i cessionari. Aquest és el principal punt d'interès, ja que la llei pretén evitar que es facin cessions que tinguin poc o res a veure amb l'àmbit de les funcions, atribucions o competències de l'organització cedent i l'organització cessionària.

- El previ consentiment informat de la persona interessada; és a dir, que abans de procedir a la cessió, l'organització ha d'aconseguir el consentiment informat de l'interessat per efectuar la cessió de les seves dades, i l'ha d'informar de les qüestions següents:
  - Identificació, activitat i adreça del cessionari.
  - Finalitat a la qual es destinaran les dades cedides.

El mateix article estableix supòsits taxats en els quals no serà preceptiu informar els interessats i aconseguir-ne el consentiment previ per a cedir les dades:

- Quan la cessió estigui autoritzada per una llei. Així, trobem supòsits en els quals estan permeses les cessions de dades com en la Llei general tributària i en la Llei d'enjudiciament civil.

- Quan es tracti de dades recollides de fonts accessibles al públic, sempre que el tractament de les dades sigui necessari per a la satisfacció de l'interès legítim perseguit pel cedent o pel cessionari i es respectin els drets dels interessats.

- Quan el tractament respongui a la lliure i legítima acceptació d'una relació jurídica el desenvolupament, compliment i control de la qual impliqui necessàriament connexió d'aquest tractament amb fitxers de tercers. En aquest cas, la comunicació només és legítima quan es limiti a la finalitat que la justifiqui.

- Quan la comunicació que s'hagi d'efectuar tingui per destinatari el defensor del poble, el Ministeri Fiscal o els jutges o tribunals o el Tribunal de Comptes en l'exercici de les funcions que té atribuïdes. Tampoc no caldrà el consentiment quan la comunicació tingui com a destinatari institucions autonòmiques amb funcions anàlogues al defensor del poble o al Tribunal de Comptes.

- Quan la cessió es produeixi entre administracions públiques i tingui per objecte el tractament posterior de les dades amb finalitats històriques, estadístiques i científiques. A més, no es permeten per llei les cessions de dades entre diferents administracions públiques per a l'exercici de competències diferents o per a finalitats diferents de les que van motivar la recollida de les dades.

- Quan la cessió de dades de caràcter personal relatives a la salut sigui necessària per a solucionar una urgència que requereixi accedir a un fitxer o per a fer els estudis epidemiològics en els termes establerts en la legislació sobre sanitat estatal o autonòmica.

Deure secret

El deure secret, que es regula en l'article 10 LOPD, afecta tot el personal que té accés a les dades personals, independentment del tipus de relació que el vinculi a l'organització (és a dir, afecta tant personal laboral, com col·laboradors externs, subcontractats, becaris, etc.), bé sigui mitjançant l'accés als sistemes d'informació o bé mitjançant l'accés a la informació en paper.

L'obligació del deure secret subsisteix encara una vegada finalitzades les relacions amb el responsable del fitxer i implica que el personal no haurà de divulgar o comunicar, ni podrà fer-ho, a terceres persones la informació o les dades que maneja o de les quals tingui coneixement en l'acompliment del seu càrrec o funcions.

El personal ha de signar, bé sigui en el moment de la contractació o bé en el moment d'incorporar-se a l'organització, clàusules de confidencialitat i de deure secret.

1.3.3. Drets dels afectats

La LOPD, en el títol III, regula els drets que té el titular de les dades i que aquest pot exercir directament davant de l'organització responsable del fitxer. L'organització ha d'establir procediments interns per a garantir que s'aporta resposta dins del termini i en la forma escaient als ciutadans que sol·liciten l'exercici de drets, atès que la no-resposta en els terminis taxats per la normativa pot representar una reclamació davant l'autoritat de control competent.

Les sol·licituds d'exercici de drets han d'anar acompanyades d'una sol·licitud, dirigida a l'organització responsable del fitxer, juntament amb una fotocòpia del DNI o mitjançant qualsevol altre mitjà vàlid en dret que acrediti la identitat de la persona interessada.

Els principals drets del titular de les dades són els següents:

Dret d'accés

El dret d'accés és el dret del titular de les dades a sol·licitar i obtenir gratuïtament, de l'organització responsable del fitxer, informació de les seves dades de caràcter personal sotmeses a tractament, l'origen d'aquestes dades, i també les comunicacions que se n'ha fet o que se'n preveu fer.

L'organització, per tant, té obligació d'informar gratuïtament el ciutadà que així ho sol·liciti amb relació a les seves pròpies dades del següent:

- Dades personals que s'emmagatzemen (totes les dades de base, i també els resultats de qualsevol elaboració o procés informàtic).

- Com es van obtenir (si les dades procedeixen de fonts diverses, s'hauran d'especificar, identificant la informació que prové de cadascuna d'elles).

- Fitxers en els quals es troben.

- Finalitat i ús d'aquestes dades.

- Si han estat o van ser cedides a tercers (amb la indicació dels cessionaris d'aquestes dades).

L'organització té un mes des de la recepció de la sol·licitud per a contestar-la; la falta de contestació s'entén com a desestimació i legitima per a reclamar davant l'autoritat de control competent.

Dret de rectificació

El dret de rectificació és el dret del titular de les dades a sol·licitar a l'organització responsable del fitxer la rectificació de les seves dades personals quan siguin inexactes, incompletes, inadequades o excessives.

L'organització té l'obligació de corregir gratuïtament les dades incompletes o inexactes del ciutadà quan així ho sol·liciti.

La sol·licitud, a més d'acreditar la identitat del sol·licitant, com s'ha citat anteriorment, haurà d'anar acompanyada de la documentació que acrediti la inexactitud o incorrecció de les dades.

L'organització haurà de corregir les dades, si escau, en el termini màxim de deu dies des de la recepció de la sol·licitud.

Dret de cancel·lació

El dret de cancel·lació és el dret del titular de les dades a sol·licitar a l'organització responsable del fitxer la cancel·lació de les seves dades personals quan siguin inexactes o incompletes, inadequades o excessives, i també quan revoqui el consentiment prestat inicialment per a tractar les dades personals que li són pròpies.

És necessari indicar que la cancel·lació no és escaient quan hi ha una obligació de conservar les dades.

En el cas de les històries clíniques, tal com estableix la Llei 41/2002, hi ha l'obligació que hi figuri tota la informació que es considera transcendental per al coneixement veraç i adequat de l'estat de salut del pacient, per la qual cosa no s'han d'eliminar dades rellevants de la història.

A més, aquesta norma estableix que la documentació clínica s'haurà de conservar per a la deguda assistència al pacient durant el temps adequat a cada cas i, com a mínim, cinc anys comptadors des de la data d'alta de cada procés assistencial.

En cas que la cancel·lació sigui procedent, aquesta s'ha de fer en una termini màxim de deu dies des de la recepció de la sol·licitud.

1.4. Reglament de mesures de seguretat

La norma que estableix les mesures de caràcter tècnic i organitzatiu que han de ser adoptades per totes les organitzacions, tant públiques com privades, que emmagatzemin, tractin fitxers de dades de caràcter personal i hi accedeixin és el Reial decret 994/1999, d'11 de juny, que aprova el Reglament de mesures de seguretat per als fitxers automatitzats de dades de caràcter personal.

1.4.1. Objecte i àmbit d'aplicació

El reglament sobre mesures de seguretat té per objecte determinar les mesures tècniques i organitzatives que garanteixin la confidencialitat, integritat i disponibilitat de la informació que contingui dades personals, amb la finalitat de preservar-les enfront de la seva alteració, la pèrdua, el tractament o l'accés no autoritzat. Aquestes mesures hauran de ser adoptades i implantades per l'organització responsable del fitxer i, si escau, per l'empresa que gestioni els sistemes d'informació que tractin els fitxers.

Les mesures tècniques i organitzatives establertes pel Reglament sobre mesures de seguretat s'han d'aplicar sobre:

- Els fitxers automatitzats, entesos com qualsevol conjunt organitzat de dades de caràcter personal, qualsevol que sigui la seva forma o modalitat de creació, emmagatzematge, organització i accés.

- Els centres de tractament, entesos com els llocs habilitats on es troben els ordinadors, equips i servidors que emmagatzemen la informació.

- Els locals, entesos com els llocs on es troben físicament situats els equips i el personal que tracta dades.

- Els equips, entesos com qualsevol material en suport físic que serveixi per a tractar i emmagatzemar electrònicament dades personals.

- Els sistemes i programes informàtics que tracten les dades de caràcter personal.

- Les persones que accedeixen a les dades (personal laboral, personal subcontractat, becaris, personal en pràctiques, etc.) que, d'acord amb les seves funcions i obligacions, intervé en qualsevol de les fases del tractament de les dades.

Els fitxers en paper

En el moment de redactar aquest material, el reglament en vigor, el Reial decret 994/1999, no s'aplica als fitxers en paper, encara que es preveu l'aprovació d'un nou reglament que els comprengui.

1.4.2. Nivells de seguretat

El reglament sobre mesures de seguretat estableix tres nivells de seguretat, que tenen la consideració de mínims legals exigibles, per la qual cosa cada organització pot implantar les mesures de seguretat addicionals que consideri adequades atenent al tipus d'informació tractada, i a altres requeriments als quals pugui estar subjecta.

Els nivells de seguretat establerts són els que segueixen:

- Nivell bàsic: aplicable a tots els fitxers que continguin dades de caràcter personal.

- Nivell intermedi: aplicable als tipus de dades següents:
  - Fitxers que continguin dades relatives a la comissió d'infraccions administratives o penals.

  - Fitxers que continguin dades sobre la Hisenda pública.

  - Fitxers que continguin dades sobre serveis financers.

  - Fitxers que continguin dades sobre solvència patrimonial i crèdit.

  - Fitxers que continguin un conjunt de dades suficients que permetin elaborar un perfil de la persona afectada.

- Nivell alt: aplicable als fitxers que continguin dades d'ideologia, religió, creences, origen racial, salut, vida sexual.

Sobre els nivells de seguretat

El reglament estableix els nivells de seguretat d'una manera acumulativa; així, en cas de tractament de fitxers de nivell intermedi, s'hauran d'implantar totes i cadascuna de les mesures de seguretat descrites per al nivell bàsic i les de l'intermedi. Igualment succeirà amb els fitxers de nivell alt, que hauran d'implantar les mesures descrites per al nivell bàsic, l'intermedi i l'alt.

1.4.3. Mesures de seguretat

	Nivell bàsic	Nivell intermedi	Nivell alt
Document de seguretat / àmbit d'aplicació	• Mesures, normes, procediments regles i estàndards de seguretat. • Funcions i obligacions del personal. • Estructura i descripció de fitxers i sistemes d'informació. • Procediment de notificació, gestió i resposta davant incidències. • Procediment de realització de còpies de suport i recuperació de dades.	• Identificació del responsable de seguretat. • Control periòdic del compliment del document. • Mesures que cal adoptar en cas de reutilització o rebuig de suports.	

	Nivell bàsic	Nivell intermedi	Nivell alt
Personal	• Funcions i obligacions clarament definides i documentades. • Difusió entre el personal de les normes que l'afectin i de les conseqüències per incompliment.		
Incidències	• Registrar tipus d'incidència, moment en què s'ha produït, persona que la notifica, persona a la qual es comunica i efectes derivats.	• Registrar realització de procediments de recuperació de les dades, persona que ho executa, dades restaurades i gravades manualment. • Autorització per escrit del responsable del fitxer per a la seva recuperació.	
Identificació i autenticació	• Relació actualitzada d'usuaris i accessos autoritzats. • Procediments d'identificació i autenticació. • Criteris d'accessos. • Procediments d'assignació i gestió de contrasenyes i periodicitat amb què es canvien. • Emmagatzematge inintel·ligible de contrasenyes actives.	• S'estableix el mecanisme que permeti la identificació d'una manera inequívoca i personalitzada de qualsevol usuari i la verificació que està autoritzat. • Límit d'intents reiterats d'accés no autoritzat.	
Control d'accés	• Cada usuari accedeix únicament a les dades i als recursos necessaris per al desenvolupament de les seves funcions. • Mecanismes que evitin l'accés a dades o recursos amb drets diferents dels autoritzats. • Concessió de permisos d'accés només per personal autoritzat.	• Control d'accés físic als locals on es trobin situats els sistemes d'informació.	
Gestió de suports	• Identificar el tipus d'informació que contenen. • Inventari. • Emmagatzematge amb accés restringit. • Sortida de suports autoritzada pel responsable del fitxer.	• Registre d'entrada i sortida de suports. • Mesures per a impedir la recuperació posterior d'informació d'un suport que hagi de ser rebutjat o reutilitzat. • Mesures que impedeixin la recuperació indeguda de la informació emmagatzemada en un suport que haurà de sortir com a conseqüència d'operacions de manteniment.	• Encriptació de dades en la distribució de suports.
Còpies de suport	• Verificar la definició i aplicació dels procediments de còpies i recuperació. • Garantir la reconstrucció de les dades en l'estat en què es trobaven en el moment de produir-se la pèrdua o destrucció. • Còpia de suport, almenys setmanal.		• Còpia de suport i procediments de recuperació en lloc diferent del que es trobin els equips.

	Nivell bàsic	Nivell intermedi	Nivell alt
Responsable		• Un o diversos nomenats pel responsable del fitxer. • Encarregat de coordinar i controlar les mesures del document. • No comporta delegació de responsabilitat del responsable del fitxer.	
Proves		• Només es fan si s'assegura el nivell de seguretat corresponent al tipus de fitxer tractat.	
Auditoria		• Almenys cada dos anys, interna o externa. • Adequació de les mesures i dels controls. • Deficiències i propostes correctores. • Anàlisi del responsable de seguretat i conclusions al responsable del fitxer. • Adopció de les mesures correctores adequades.	
Registre d'accessos			• Registrar usuari, hora, fitxer, tipus d'accés i registre accedit. • Control del responsable de seguretat. Informe mensual. • Conservació durant dos anys.
Telecomunicacions			• Transmissió de dades encriptada.

1.5. Règim sancionador

1.5.1. Autoritats de control

Les autoritats de control, o agències de protecció de dades, es constitueixen com el garant de l'aplicació dels principis recollits en la normativa. A l'Estat espanyol s'estableixen dos àmbits d'actuació:

- L'Agència Espanyola de Protecció de Dades: té potestat sobre els fitxers privats en tot l'Estat espanyol.

- Agències autonòmiques: el seu àmbit competencial se circumscriu als fitxers creats o gestionats per les administracions públiques del seu àmbit territorial:
  - Agència Catalana de Protecció de Dades.
  - Datuak Babesteko Euskal Bulegoa (Agència Basca de Protecció de Dades).
  - Agència de Protecció de Dades de la Comunitat de Madrid.

Amb caràcter general, les principals funcions dels òrgans de control són les següents:

- Vetllar pel compliment de la legislació vigent sobre protecció de dades personals.
- Proporcionar informació sobre els drets de les persones en matèria de tractaments de dades personals.
- Atendre les peticions i les reclamacions formulades per les persones afectades.
- Dictar les instruccions necessàries per a adequar els tractaments als principis de la legislació.
- Exercir la potestat d'inspecció i exercir la potestat sancionadora.

1.5.2. Infraccions i sancions

Les infraccions i sancions s'aborden en el títol VII de la Llei. Concretament, l'article 44 ens diu el següent:

"**1)** Les infraccions es qualifiquen com a lleus, greus o molt greus.

2) Són infraccions lleus:

a) No atendre, per motius formals, la sol·licitud de la persona interessada de rectificació o cancel·lació de les dades personals objecte de tractament quan legalment sigui procedent.

b) No proporcionar la informació que sol·liciti l'Agència Espanyola de Protecció de Dades en l'exercici de les competències que té legalment atribuïdes, amb relació a aspectes no substantius de la protecció de dades.

c) No sol·licitar la inscripció del fitxer de dades de caràcter personal en el Registre General de Protecció de Dades, quan no sigui constitutiu d'infracció greu.

d) Procedir a la recollida de dades de caràcter personal dels mateixos afectats sense proporcionar-los la informació que assenyala l'article 5 d'aquesta llei.

e) Incomplir el deure secret establert en l'article 10 d'aquesta llei, tret que constitueixi una infracció greu.

3) Són infraccions greus:

a) Procedir a la creació de fitxers de titularitat pública o iniciar la recollida de dades de caràcter personal per a aquests fitxer, sense autorització de disposició general, publicada en el Butlletí Oficial de l'Estat o diari oficial corresponent.

b) Procedir a la creació de fitxers de titularitat privada o iniciar la recollida de dades de caràcter personal per als fitxers amb finalitats diferents de les que constitueixen l'objecte legítim de l'empresa o entitat.

c) Procedir a la recollida de dades de caràcter personal sense aconseguir el consentiment exprés de les persones afectades, en casos en què aquest sigui exigible.

d) Tractar les dades de caràcter personal o usar-les posteriorment amb conculcació dels principis i garanties establerts en aquesta llei o amb incompliment dels preceptes de protecció que imposin les disposicions reglamentàries de desenvolupament, quan no constitueixi infracció molt greu.

e) L'impediment o l'obstaculització de l'exercici dels drets d'accés i oposició i la negativa a facilitar la informació que sigui sol·licitada.

f) Mantenir dades de caràcter personal inexactes o no efectuar-ne les rectificacions o cancel·lacions que legalment escaiguin quan resultin afectats els drets de les persones que aquesta llei empara.

g) La vulneració del deure de guardar secret sobre les dades de caràcter personal incorporades a fitxers que continguin dades relatives a la comissió d'infraccions administratives o penals, Hisenda pública, serveis financers, prestació de serveis de solvència patrimonial i crèdit, i també aquells altres fitxers que continguin un conjunt de dades de caràcter personal suficients per a obtenir una avaluació de la personalitat de l'individu.

h) Mantenir els fitxers, locals, programes o equips que continguin dades de caràcter personal sense les degudes condicions de seguretat que per via reglamentària es determinin.

i) No remetre a l'Agència Espanyola de Protecció de Dades les notificacions previstes en aquesta llei o en les seves disposicions de desenvolupament, i no proporcionar-hi en termini tots els documents i les informacions hagi de rebre o que requereixi a aquest efecte.

j) L'obstrucció a l'exercici de la funció inspectora.

k) No inscriure el fitxer de dades de caràcter personal en el Registre General de Protecció Dades, quan hagi estat requerit per a això pel director de l'Agència Espanyola de Protecció de Dades.

l) Incomplir el deure d'informació que s'estableix en els articles 5, 28 i 29 d'aquesta llei, quan les dades hagin estat recollides per una persona diferent de l'afectada.

4) Són infraccions molt greus:

a) La recollida de dades en forma enganyosa i fraudulenta.

b) La comunicació o cessió de les dades de caràcter personal, excepte en els casos en què estiguin permeses.

c) Recollir i tractar les dades de caràcter personal a què es refereix l'apartat 2 de l'article 7 quan no intervingui el consentiment exprés de la persona afectada; recol·lectar i tractar les dades referides en l'apartat 3 de l'article 7 quan no ho disposi una llei o la persona afectada no ho hagi consentit expressament, o violentar la prohibició continguda en l'apartat 4 de l'article 7.

d) No cessar en l'ús il·legítim dels tractaments de dades de caràcter personal quan sigui requerit per a això pel director de l'Agència Espanyola de Protecció de Dades o per les persones titulars del dret d'accés.

e) La transferència temporal o definitiva de dades de caràcter personal que hagin estat objecte de tractament o hagin estat recollides per sotmetre-les a aquest tractament, amb destinació a països que no proporcionin un nivell de protecció equiparable sense autorització del director de l'Agència Espanyola de Protecció de Dades.

f) Tractar les dades de caràcter personal d'una manera il·legítima o amb menyspreu dels principis i garanties que els siguin aplicables, quan amb això s'impedeixi o s'atempti contra l'exercici dels drets fonamentals.

g) La vulneració del deure de guardar secret sobre les dades de caràcter personal a què fan referència els apartats 2 i 3 de l'article 7, i les que hagin estat recollides per a finalitats policials sense consentiment de les persones afectades.

h) No atendre o obstaculitzar d'una manera sistemàtica l'exercici dels drets d'accés, rectificació, cancel·lació o oposició.

i) No atendre d'una manera sistemàtica el deure legal de notificació de la inclusió de dades de caràcter personal en un fitxer."

Pel que fa a les sancions, cal comentar que el règim sancionador de la LOPD és dels més severs de l'entorn europeu. Així, en l'article 45, la LOPD estableix el següent:

"**1)** Les infraccions lleus han de ser sancionades amb una multa de 601 a 60.101 euros.

2) Les infraccions greus han de ser sancionades amb una multa de 60.101 a 300.506 euros.

3) Les infraccions molt greus han de ser sancionades amb una multa de 300.506 a 601.012 euros."

L'article 46 de la llei fa un esment especial de les infraccions comeses en fitxers dels quals siguin responsables les administracions públiques.

"**1)** Quan les infraccions a les quals es refereix l'article 44 siguin comeses en fitxers dels quals siguin responsables les administracions públiques, el director de l'Agència Espanyola de Protecció de Dades dicta una resolució establint les mesures que escaigui adoptar perquè cessin o es corregeixin els efectes de la infracció. Aquesta resolució s'ha de notificar al responsable del fitxer, a l'òrgan del qual depengui jeràrquicament i a les persones afectades, si n'hi hagués.

2) El director de l'agència també pot proposar la iniciació d'actuacions disciplinàries, si fossin procedents. El procediment i les sancions que cal aplicar són les establertes en la legislació sobre règim disciplinari de les administracions públiques.

3) S'hauran de comunicar a l'agència les resolucions que pertoquin amb relació a les mesures i actuacions a què es refereixen els apartats anteriors."

És a dir, en el cas de les administracions públiques, les infraccions no comporten cap sanció econòmica.

2. Introducció als elements tècnics de models de seguretat

2.1. Fonaments de seguretat tècnica

Es diu que una cosa és segura quan no és susceptible de fallar en qualsevol dels sentits o al·lusions cap a aquest objecte o afirmació. La *seguretat* és un concepte que transcendeix la major part de les activitats humanes.

En aquest sentit, hem de tenir en compte dos aspectes:

- Sempre que hi hagi un bé per protegir, cal dedicar temps i recursos a neutralitzar les possibles amenaces que pugui sofrir per mitjà del que anomenem *mecanismes de seguretat*.

- La tecnologia associada al processament de dades s'ha convertit en un element essencial en les nostres vides. La informàtica ha passat a ser una cosa sense la qual és impossible concebre certs aspectes de l'actualitat, tant científica com civil.

La combinació dels dos aspectes anteriors ens indica ja la importància que té la seguretat informàtica en les nostres vides. Cada vegada amb més freqüència es delega als equips informàtics la responsabilitat de la gestió de productes, persones, vots, informació en general. A causa d'això, cada vegada és més gran la possibilitat que es produeixin errors en la gestió de la informació:

- Augmentarà la gravetat dels errors en la gestió.
- Augmentarà el benefici extraïble dels errors.
- Augmentarà el nombre de persones interessades que es produeixin errors.

A part de l'indicat anteriorment, hi ha altres factors que fan de la seguretat informàtica una disciplina particularment difícil:

- Es poden ocasionar molts danys a distància, amb un risc mínim per qui els provoca.

- L'equip necessari per a exercir la delinqüència informàtica té un cost relativament baix.

- És possible, encara que difícil, esborrar qualsevol petjada del delicte.

- No hi ha una formació sòlida sobre els sistemes que cal administrar, a causa de la seva complexitat i del seu avenç ràpid.

- La legislació no va a l'una amb els avenços informàtics i hi ha dificultats per a aplicar les lleis existents.

- Els delictes no sempre són denunciats per les organitzacions a causa de la publicitat adversa que es pot generar.

Un agreujant

Per si això fos poc, cada vegada amb més freqüència els mitjans de comunicació, especialitzats o no, donen a conèixer casos de frau, espionatge, destrucció de la propietat intel·lectual, sabotatge, intrusió, robatori, plagi o competència deslleial, relacionats amb el món de la informàtica.

Aquests successos els pot ocasionar un empleat venjatiu, un administrador ineficaç, un intrús informàtic, un usuari irresponsable, programari mal desenvolupat o una catàstrofe natural. Els seus blancs poden estar perfectament seleccionats o ser totalment aleatoris, de conseqüències immediates o solament visibles amb el pas del temps, però tots es tradueixen en pèrdues de temps i diners per a les empreses que els sofreixen.

Fins a l'aparició de la informàtica, la valoració dels actius d'una empresa es feia segons els objectes físics útils, les produccions pròpies, les infraestructures, la tresoreria i el capital humà. Des de la seva aparició, la informació ha cobrat un valor com a capital. No és que abans no hi hagués informació a les empreses, l'espionatge industrial és tan antic com la Revolució Industrial, però es mantenia amb el sistema de paper i arxivadors i formava part dels actius de l'oficina. Avui dia, es maneja una quantitat ingent d'informació de procedències molt diverses. El valor afegit d'una empresa pot ser la informació que maneja.

En conseqüència, cada vegada és més important mantenir la seguretat de la informació, però també és més difícil perquè els riscos són més grans.

Podem identificar tres tipus de riscos, segons l'origen:

- errors involuntaris de persones i/o màquines,
- desastres naturals,
- atacs voluntaris.

Els errors involuntaris són les amenaces més comunes: sobre el 80% dels casos. Els problemes creats per aquests es poden classificar en dues famílies:

- Denegació de servei: no-disponibilitat dels recursos.

- Observació no autoritzada (atac a la confidencialitat): accés a la informació i la seva modificació ja sigui esborrant, afegint o substituint dades.

La protecció de la informació és més difícil des de l'aparició de les xarxes telemàtiques. Aquestes xarxes, i especialment Internet, fan que la informació sigui un problema global i no aïllat a les màquines internes de l'empresa. Les tecnologies aplicades a la seguretat en xarxes es troben en la fase de desenvolupament inicial, especialment per dos motius:

- La majoria dels sistemes operatius estan pensats per a arquitectures ordinador central / terminal i no per a arquitectures client/servidor o Internet/intranet que s'utilitzen actualment.

- No hi ha estàndards ni organitzacions mundials acceptats per totes les empreses proveïdores de seguretat.

En dissenyar un sistema de seguretat per a una empresa s'ha de tenir en compte que **no** existeix un sistema completament segur. Entre els informàtics se sol comentar el següent: "Un ordinador segur és aquell que està desconnectat de la Xarxa, enterrat en un búnquer de formigó, diversos metres sota terra, amb un guàrdia de seguretat a la porta..., i així i tot no és possible garantir que estigui completament segur".

En general, per a protegir la informació s'utilitzen els serveis de seguretat següents:

- Autenticació. Autenticar un usuari és comprovar que és qui declara ser. L'autenticació es pot dur a terme actualment amb diferents mètodes. El més comú és el d'inici de sessió (*login*) i contrasenya (*password*), però també hi ha els testimonis (*tokens*), les targetes intel·ligents (*smart cards*), sistemes biomètrics, els certificats digitals, etc.

- Control d'accessos. El control d'accessos consisteix a protegir la informació contra accessos no volguts, tant físics com lògics.

- Confidencialitat. La confidencialitat és la capacitat de mantenir en secret el contingut d'un document.

- Integritat. La integritat consisteix a garantir que el contingut d'un document no ha estat alterat o modificat.

- No-repudi. El no-repudi evita que una persona pugui negar que ha fet una acció quan l'ha fet.

- Disponibilitat. La disponibilitat consisteix a assegurar el funcionament de tots els recursos.

2.1.1. Nivells de seguretat

Podem identificar tres nivells de seguretat, que desenvoluparem en els apartats següents:

Seguretat física

Per *seguretat física* podem entendre tots aquells mecanismes, generalment de prevenció i detecció, destinats a protegir físicament qualsevol recurs del sistema.

Exemples de recursos que cal protegir

Entenem per *recursos que cal protegir* des d'un simple teclat fins a una cinta de còpia de seguretat (*backup*) amb tota la informació que hi ha en el sistema, passant per la mateixa CPU de la màquina.

En moltes organitzacions se solen prendre mesures per a prevenir o detectar accessos no autoritzats o denegacions de servei, però rares vegades per a prevenir l'acció d'un atacant que intenta accedir físicament a la sala d'operacions o al lloc on es dipositen les impressions del sistema.

Això motiva que, en determinades situacions, un atacant s'inclini per aprofitar vulnerabilitats físiques, ja que li pot resultar més fàcil robar una cinta amb una imatge completa del sistema que intentar accedir-hi a partir d'errors del programari.

El nivell de seguretat física depèn completament de l'entorn en què se situïn els punts que cal protegir.

A continuació, enumerarem diferents perills que afecten la seguretat física:

- **Desastres naturals**. Els desastres naturals no són massa freqüents, però quan succeeixen, acostumen a implicar conseqüències gravíssimes, a causa, sobretot, de la falta de prevenció.
  - Les tempestes amb aparell elèctric, especialment freqüents a l'estiu (quan molt personal es troba de vacances, la qual cosa les fa més perilloses), generen pujades de tensió sobtades infinitament superiors a les que pugui generar un problema a la xarxa elèctrica. Si cau un raig sobre l'estructura metàl·lica de l'edifici on estan situats els equips, és gairebé segur que en caldrà comprar altres de nous. Sense arribar a ser tan dramàtics, la caiguda d'un raig als voltants d'un edifici amb material informàtic pot induir un camp magnètic prou intens per a destruir maquinari fins i tot protegit contra voltatges elevats.

  - Les inundacions. En moltes empreses el centre de processament de dades és al soterrani, ja que és un lloc poc accessible per no disposar de finestres per les quals puguin entrar els possibles lladres. Però els soterranis són especialment vulnerables davant les inundacions. Atès que la ubicació dels equips ja sol estar decidida quan es pensa en les mesures de seguretat, caldrà utilitzar mesures de detecció, com, per exemple, detectors d'aigua als sòls o falsos sòls de les sales d'operacions que provoquin l'apagada dels equips en cas que s'activin.

- **Desastres de l'entorn**. Entre els més freqüents podem destacar les pujades o baixades de tensió, el corrent estàtic, incendis, accessos físics no autoritzats o robatoris de dades.
  - Canvis de tensió. La manera més efectiva de protegir equips contra els canvis de tensió és utilitzar un SAI (sistema d'alimentació ininterrompuda).

  - Corrent estàtic. Aquest és un fenomen estrany que la majoria de gent pensa que no afecta els equips, només altres persones. Res més lluny de la realitat: simplement tocar amb la mà la part metàl·lica de teclat o un conductor d'una placa pot destruir completament un equip. Contra el problema del corrent estàtic hi ha moltes solucions i molt barates: esprai antiestàtic, ionitzadors antiestàtics, etc.

  - Incendis. Els incendis solen estar molt relacionats amb l'electricitat (la causa del foc pot ser també, evidentment, un desastre natural): la sobrecàrrega de la xarxa a causa del gran nombre d'aparells connectats a la línia, un simple curtcircuit o un equip que s'escalfa massa es poden convertir en la causa directa d'un incendi.

  - Accés físic no autoritzat. Hem de tenir en compte que, encara que una part dels equips sol estar ben protegida davant accessos físics no autoritzats, com els servidors, molts equips seran en llocs semipúblics als quals és fàcil accedir (i discret) i des dels quals és també fàcil llançar un atac complet sobre la xarxa. S'ha d'extremar la protecció de tots els equips davant aquests accessos no autoritzats.

  - Robatori de dades. La seguretat física també implica una protecció de la informació del nostre sistema, tant de la que hi està emmagatzemada com de la que es transmet entre diferents equips. De tota manera, hi ha certs aspectes que s'han de tenir en compte en dissenyar una política de seguretat física que afecten principalment, a part dels elements físics, les dades d'una organització: alguns atacs tenen com a objectiu no destruir el medi físic del nostre sistema, sinó simplement aconseguir la informació que hi ha emmagatzemada.
    Un error molt habitual és emmagatzemar els dispositius de còpia de seguretat en llocs molt propers a la sala d'operacions, o fins i tot a la mateixa sala. Això, que en principi pot semblar correcte (i còmode si es necessiten restaurar uns arxius) es pot convertir en un problema: un mateix atac podria fer que es perdessin tant els equips com les dades (els de els mateixos equips i els de la còpia de seguretat). És recomanable guardar les còpies de seguretat en una zona allunyada de la sala d'operacions, encara que això impliqui duplicar els sistemes de seguretat.

Seguretat en el nivell d'enllaç-xarxa-transport

La seguretat d'una xarxa depèn, en gran manera, dels nivells OSI enllaç, xarxa i transport.

Per introduir-se a les xarxes, els atacants solen aprofitar problemes en el disseny de la topologia de les xarxes i en els protocols d'encaminament entre els diferents elements. Per tant, aquests són els punts sobre els quals un administrador de sistemes ha de prestar especial atenció.

- Seguretat en dispositius de xarxa. Els dispositius de xarxa (commutadors -*switches*-, encaminadors, concentradors -*hubs*-, balancejadors de càrrega, etc.) són els punts febles de qualsevol xarxa, són els responsables de la topologia de xarxa resultant i, per tant, una variació en la seva configuració pot afectar tota la xarxa.

Vulnerabilitat dels dispositius de xarxa

Aquests dispositius tenen diferents maneres d'administració, però bàsicament la seva administració remota es basa en un protocol una mica desfasat quant a seguretat com és l'SNMP.

- Vulnerabilitats en la pila TCP/IP. En l'època en la qual es va dissenyar el protocol TCP/IP, es va tenir més en compte la seva estabilitat i el seu rendiment que la seguretat, qüestió que mancava d'importància en el disseny preliminar. Avui dia és un dels protocols de xarxa més utilitzats i el responsable de la xarxa Internet.

Identificació d'equips

En un servidor podem tenir diversos ports o serveis que escolten. La manera més simple de representar aquesta situació és l'adreça IP de l'equip seguida del nombre identificador del port. Per exemple, 172.16.1.123:80 és el servei web de l'equip amb IP 172.16.1.123.

- Encaminadors i tècniques d'encaminament. S'entén per *encaminament* la funció que fa arribar paquets d'informació d'una màquina a una altra, sense tenir en compte ni el mitjà físic ni la qualitat de les dades que es transmeten. Perquè això es dugui a terme, el sistema emissor ha de saber quins altres sistemes són a la seva mateixa xarxa i on ha d'enviar les dades en cas que la màquina no pertanyi al seu entorn directe.

- Servidors intermediaris (*proxies*). Un servidor intermediari és un sistema de programari d'intermediari entre dues xarxes, que permet regular el trànsit de sortida i entrada entre elles a partir d'un únic ordinador central (*host*), i es gestionen d'aquesta manera tant el trànsit com el contingut de les comunicacions entre els dos entorns. Generalment, un servidor intermediari de sessió permet a equips d'una xarxa local connectar-se a una altra xarxa, per exemple, a equips d'Internet, per mitjà d'un únic equip i d'una única connexió a Internet.

- *Firewall* o tallafocs, és un sistema, ja sigui maquinari o programari, que s'encarrega de filtrar el trànsit TCP/IP generalment entre xarxes; per exemple, entre Internet i una xarxa local d'una oficina. Per tant, el tallafocs filtrarà el trànsit entrant des d'Internet (una xarxa no fiable) cap a la LAN (la

nostra xarxa), i permetrà el trànsit sortint des de la LAN cap a Internet. A un nivell molt senzill, un tallafocs de xarxa pot evitar, i fins i tot bloquejar, l'extensió d'un atac.

- Detectors (*sniffers*). Són dispositius que capturen paquets de la xarxa. El seu ús legítim és analitzar el trànsit de xarxa i identificar les àrees més preocupants en potència. Per exemple, si un segment de la xarxa té un rendiment baix s'usarà un detector per a determinar la causa d'una manera precisa.
  Els detectors són perillosos perquè poden capturar contrasenyes, informació confidencial o propietària, i poden ser usats per a traspassar la seguretat de xarxes interconnectades o per a guanyar privilegis. De fet, l'existència d'un detector no autoritzat a la xarxa indicarà que la seguretat està realment compromesa.

- Tunelització (*tunneling*). La necessitat de seguretat fa que cada vegada sigui més comú l'ús de VPN (xarxes virtuals privades). Aquestes xarxes s'implementen per mitjà d'un protocol anomenat *PPTP* (*point to point tunneling protocol*) que assegura trànsit encriptat entre punts d'enllaç corporatius basant-se en una xarxa de treball via TCP/IP. Això elimina la necessitat de línies pròpies o llogades i també el perill de l'*sniffing*.

Seguretat en el nivell d'aplicació

- Codi maliciós - virus. En general podem dir que un virus informàtic és un petit programa dissenyat per a alterar el funcionament d'un ordinador.
  Un concepte més complet de *virus informàtic* seria el d'un petit programa capaç d'autoreproduir-se. El qualifiquem de *maliciós* perquè està dissenyat per a danyar sistemes informàtics, alterant-ne la forma de treballar o danyant informació emmagatzemada en el disc dur, sense el coneixement o permís de la persona afectada. En termes més tècnics, un *virus* es defineix com una porció de codi de programació l'objectiu del qual és implementar-se a si mateix en un arxiu executable i multiplicar-se sistemàticament d'un arxiu a un altre. A més, els virus estan dissenyats per a fer una acció concreta en els sistemes informàtics. Aquesta acció pot anar des de la simple aparició d'un missatge a la pantalla, fins a la destrucció de tota la informació continguda en el sistema.
  Els virus tenen rutines de destrucció de dades que s'activaran quan succeeixin certes condicions. Alguns virus s'activen en una data determinada.
  La fase de descobriment no té per què produir-se després de l'activació, però usualment succeeix així. Això es produeix quan algú dóna la notícia d'un nou virus. Generalment passa a les mans de la National Computer Security Association (NCSA) que es documenta i després es distribueix als dissenyadors d'antivirus.

- Vulnerabilitats de codi. A l'hora d'assegurar un sistema, no s'ha d'oblidar el codi que executa per a dur a terme les seves funcions assignades. Sempre

hi ha determinat grau de divergència entre el disseny dels programes i la seva implementació; aquestes petites diferències poden fer que un determinat programari sigui insegur, o que eines específiques de seguretat no compleixin la seva funció com ho haurien de fer.
Encara que aquestes vulnerabilitats depenen de l'ús que es faci del llenguatge de programació, cada llenguatge és susceptible enfront de determinats errors; cal conèixer-los i evitar-los. Per a localitzar aquests errors, es recorre a l'enginyeria inversa. Aquesta tècnica consisteix a descompilar el codi i observar quines vulnerabilitats són explotables per l'atacant. Un determinat programa d'atac, per a un programa objectiu específic i sobre un sistema operatiu concret, es denomina *exploit*. I la resposta a aquest *exploit* (per a neutralitzar-lo), per part de la companyia propietària del programari atacat, es denomina *pedaç* o *patch*.

2.2. Signatura electrònica i criptografia

2.2.1. Identificació i autenticació

Ja hem explicat en què consisteix l'autenticació. I sabem que és imprescindible per a poder-nos relacionar per mitjans electrònics: en primer lloc, hem d'identificar amb qui ens relacionem, i probablement dotar d'algun element de seguretat aquesta identificació (una contrasenya, una targeta o un certificat) per a ser capaços de comprovar-ne la identitat cada vegada que vulguem establir una nova transacció.

En general, cada usuari tindrà el seu propi identificador que hauria de ser únic; no es permet que diversos usuaris comparteixin un identificador. Tot identificador d'un sistema ha de tenir el seu propietari, el qual serà responsable de les accions que s'hi facin.

Fins a la data s'han vingut emprant, i es continuen emprant, noms d'usuari i contrasenyes, encara que s'aprecia un avenç dels sistemes basats en signatura electrònica i certificats reconeguts, especialment a causa de la sensibilitat del sector sanitari per a tractar dades amb exigència de seguretat de nivell alt i a la nova regulació administrativa de la signatura electrònica.

Un certificat electrònic és, senzillament, un document electrònic signat, que garanteix a les terceres persones que el reben o que l'utilitzen una sèrie de manifestacions contingudes en el document que es poden referir a la identitat d'una persona, a la titularitat o possessió d'una clau pública (i de la clau privada corresponent) dels seus privilegis (en forma de rols o perfils) o a la seva capacitat de representar una altra persona física o jurídica.

Exemple de certificat electrònic

L'exemple més clar de certificat electrònic és el certificat reconegut de clau pública per a la identificació i la signatura de les persones físiques i jurídiques.

2.2.2. Nocions bàsiques de criptografia

La criptografia és la tècnica que permet convertir un text intel·ligible (*plaintext*), en un altre, anomenat *criptograma* (*ciphertext*), el contingut d'informació del qual és igual a l'anterior però només el poden entendre les persones autoritzades.

El procés que s'aplica a les dades perquè siguin incomprensibles es denomina *encriptació*. Atès que la funció inversa (la que permetria recuperar el text intel·ligible) únicament la coneixen les persones autoritzades, l'encriptació permet assegurar la confidencialitat de les dades.

El certificat digital, compost d'una clau pública i una clau privada, és un dels mètodes que permet encriptar un document. Per a això és necessari que tant l'emissor com el receptor disposin d'aquest certificat.

La certificació digital funciona mitjançant criptografia asimètrica; és a dir, el que s'ha codificat amb una clau privada necessita la seva clau pública corresponent per a ser descodificat, i a l'inrevés.

Funcionament dels sistemes de clau pública

Els sistemes d'encriptació de clau pública es basen en funcions parany d'un sol sentit que aprofiten propietats particulars, per exemple les dels nombres primers.

Una funció d'un sol sentit és aquella la computació de la qual és fàcil, mentre que la seva inversió resulta extremament difícil. Per exemple, és fàcil multiplicar dos nombres primers junts per a obtenir un compost, però és difícil factoritzar un compost en els seus components primers.

Una funció parany d'un sentit és alguna cosa semblant, però té un "parany". Això vol dir que si es conegués alguna peça de la informació, seria fàcil computar-ne l'invers. Per exemple, si tenim un nombre compost per dos factors primaris i coneixem un dels factors, és fàcil computar-ne el segon.

Infraestructura de clau pública

La infraestructura de clau pública o PKI (*public key infrastructure*) és el sistema tècnic, jurídic, de seguretat i d'organització dels serveis de certificació i de signatura electrònica.

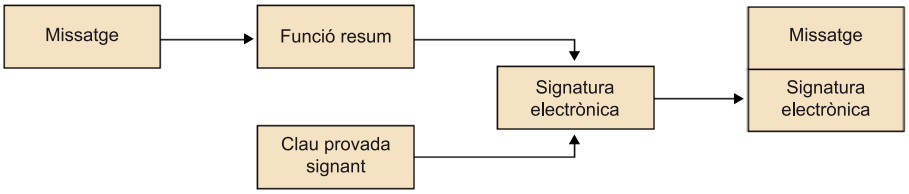
La infraestructura es diu *de clau pública* perquè les operacions de signatura i encriptació requereixen com a element fonamental la publicació i distribució de les claus públiques dels usuaris dels serveis, en forma de certificats electrònics de clau pública.

La comunicació encriptada requereix que el document s'encripti mitjançant la clau pública de la persona que es vol que el pugui llegir. Aquest document solament podrà ser desxifrat per la persona que té la clau privada complementària.

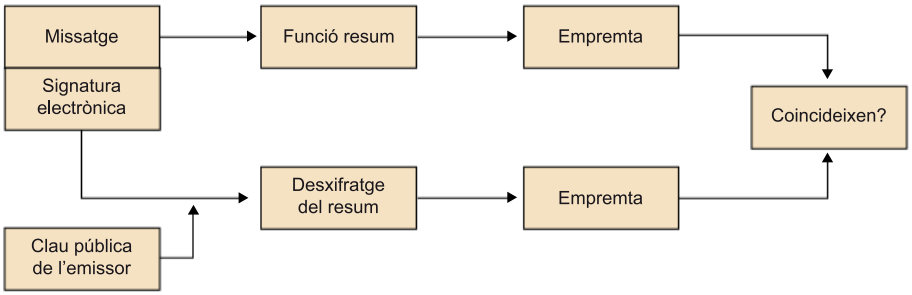
- La clau privada és secreta i només la té l'usuari. Amb ella pot signar documents electrònics.

- La clau pública està a la disposició de qualsevol usuari. Permet validar una signatura digital generada amb la clau privada complementària.

Per a generar una signatura digital, és necessari aplicar una funció resum (*hash*), mitjançant la qual s'obté l'"empremta digital" de qui vol signar el missatge. Després, la clau privada de l'usuari encripta aquesta petjada i dóna com a resultat la signatura digital del document o missatge.



Qui necessiti validar la signatura del missatge o document pot comprovar que aquest no ha estat modificat aplicant la funció de resum per a generar l'empremta, i comparar-la amb la que ha rebut.



2.2.3. Validesa legal i regulació de la signatura electrònica

La legislació sobre signatura electrònica determina en l'article 3.4 que sota el compliment de determinats requisits, "la signatura electrònica reconeguda ha de tenir, respecte de les dades consignades en forma electrònica, el mateix valor que la signatura manuscrita amb relació als consignats en paper".

S'ha de fer la distinció entre els diferents tipus de signatura electrònica que distingeix la normativa:

- Signatura electrònica, respecte de la qual s'estableix que no se li han de negar efectes jurídics, ni ha de ser exclosa com a prova en judici.

- Signatura electrònica avançada, a la qual no se li atorga un reconeixement específic encara que, evidentment, ha de tenir un valor molt més alt que

l'anterior, atès que, en virtut dels mecanismes criptogràfics empleats, dota els documents d'autenticitat i integritat.

- Signatura electrònica reconeguda que, en estar basada en un certificat reconegut i haver estat generada amb un dispositiu segur de creació de signatura, s'hauria d'equipar a la signatura manuscrita. Els certificats reconeguts són els certificats expedits per un prestador de serveis de certificació, que compleix una sèrie de requisits establerts en la llei quant a la comprovació de la identitat i altres circumstàncies dels sol·licitants i a la fiabilitat i les garanties dels serveis de certificació.

Cal destacar que el fet que la signatura reconeguda sigui equiparable a la signatura manuscrita implica que la capacitat probatòria de la signatura electrònica reconeguda és més gran que la de les altres dues modalitats, però sense que aquestes perdin aquesta capacitat.

2.3. Pla director de seguretat

El funcionament intern i la imatge davant els clients d'una empresa, o davant els ciutadans en el cas de l'Administració, depenen en gran manera del funcionament continuat dels seus sistemes d'informació entre els quals podem destacar:

- el correu i les agendes electròniques, i també l'arxivament de documents;
- els web i els procediments de tramitació.

Hem de tenir en compte que moltes empreses i institucions disposen de sistemes d'informació que tracten dades sensibles i que, a més, requereixen mesures de seguretat importants, ja que són dades que necessiten un nivell de seguretat alt.

L'objectiu d'una anàlisi de riscos és identificar totes les dades i tots els processos d'una determinada organització la sensibilitat/criticitat de la qual és important per al desenvolupament de les seves funcions.

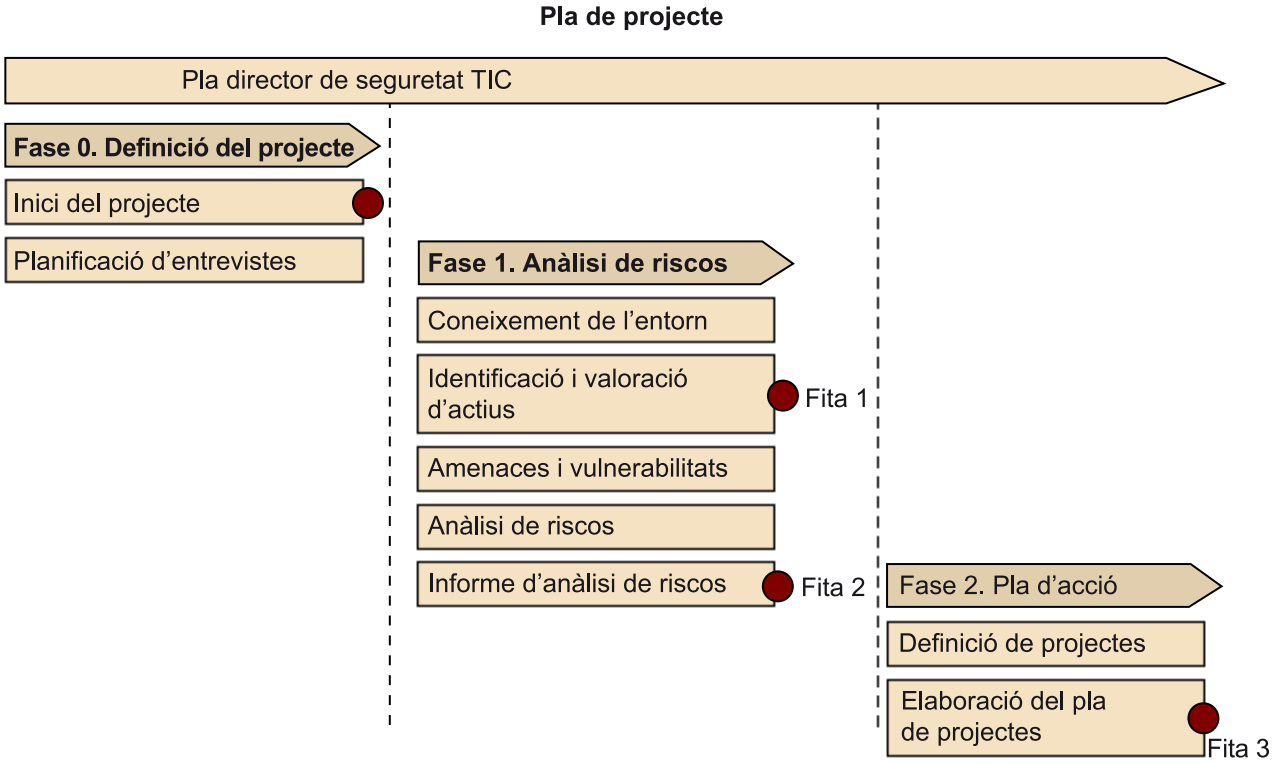
Normalment, la informació necessària per a dur a terme una anàlisi de riscos es recull mitjançant entrevistes amb els responsables de l'entitat, i l'enfocament és d'autoavaluació assistida.

L'anàlisi de riscos i la classificació de les dades i els processos es pot fer amb diferent nivell de detall. És útil concretar un primer nivell i enfocar l'estudi a la identificació dels riscos més significatius. Per tant, es pot fer la valoració del compliment dels controls recollits en la norma de pràctiques de seguretat (ISO17799).

La gestió del risc consisteix a equilibrar el cost de la protecció amb el cost d'exposició (vulnerabilitats), de manera que es minimitzi el risc.

Les fases d'una anàlisi de riscos són les següents:

- coneixement del sistema actual,
- identificació i valoració d'actius,
- amenaces i vulnerabilitats,
- anàlisi de riscos,
- informe del projecte.



Fases d'un pla director de seguretat

Qualsevol anàlisi de riscos comença per la **descripció de l'organització**, dels processos que es tracten i dels sistemes d'informació que han desenvolupat.

A continuació, es fa l'inventari **d'actius**[1] i els seus requisits de seguretat. És útil representar els actius amb una jerarquia o **arbre d'actius**, en què s'identifiquen les dependències dels diferents elements que comprèn un actiu d'informació. En l'arbre d'actius es representen les aplicacions, els elements de xarxa o els edificis on hi ha els centres de processament de dades.

Exemple de dimensions de seguretat

Les dimensions de seguretat més utilitzades són la confidencialitat, la integritat i la disponibilitat.

(1)Entenem per *actiu d'informació* la informació o el conjunt d'informacions significatives i necessàries per al desenvolupament dels diferents processos de negoci.

Un actiu d'informació és independent dels diferents elements de tractament o emmagatzematge; és a dir, de les aplicacions, base de dades, suports, edificis on se situïn els sistemes, les xarxes de comunicacions, etc.

Seguidament, es duu a terme l'anàlisi d'**amenaces i vulnerabilitats** dels actius d'informació. Per a la classificació de les vulnerabilitats es pot seguir la norma UNE ISO/IEC 17799:2005 en els seus onze apartats:

- política de seguretat;
- organització de la seguretat de la informació;
- gestió d'actius;
- seguretat dels recursos humans;
- seguretat física i mediambiental;
- gestió de les telecomunicacions i operacions;
- control d'accessos a les dades;
- adquisició, desenvolupament i manteniment dels sistemes d'informació;
- gestió d'incidències;
- gestió de la continuïtat de les operacions de l'empresa;
- conformitat.

En les anàlisis de riscos es poden incloure tests d'intrusió (accés a la informació explotant les vulnerabilitats oposades per a provar d'una manera fefaent que un atacant les podria utilitzar) per a preservar la confidencialitat de la informació, amb l'objectiu d'identificar els riscos següents:

- indisponibilitat del sistema,
- accés no autoritzat,
- incompliment del Reglament de mesures de seguretat LOPD.

Nota

L'anàlisi de riscos pot o no cobrir els requisits de l'auditoria bianual que marca la normativa de seguretat i pot comportar, o no, proves d'auditoria.

L'anàlisi de vulnerabilitats davant atacs de l'exterior pot comprendre:

- Les connexions a Internet, les connexions sense fil i els webs.
- Els components i les seves possibles vulnerabilitats significatives.
- La configuració dels punts d'accés sense fil.
- La infraestructura (encaminadors, tallafocs, servidors web, servidors d'aplicatius, etc.).
- Les aplicacions.
- El personal tècnic i els usuaris: atacs d'enginyeria social.

Seguint les directrius marcades pels resultats de l'anàlisi de riscos i tenint en compte les recomanacions associades a cada vulnerabilitat, es defineix el **pla de projectes**.

Els projectes sense un conjunt de recomanacions identificades en l'anàlisi de riscos i agrupades per a facilitar-ne l'execució.

Per a l'execució dels projectes identificats, s'estableix una priorització, conforme a les dependències que hi pugui haver entre ells, i es proposa un pla d'acció d'acord amb les necessitats i els requisits de l'organisme.

Per a cada projecte s'analitza la disminució del risc que la seva realització comporta i també es pot mostrar l'evolució en el compliment de la norma ISO 17799 que significa. És imprescindible descriure d'una manera detallada les activitats de cada projecte, i també la seva durada i els seus costos.

3. Annexos

3.1. Legislació

- Europea
  - 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.

- Estatal
  - Constitució espanyola de 1978

  - Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

  - Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

  - Reial decret 428/1993, de 26 de març, pel qual s'aprova l'Estatut de l'Agència Espanyola de Protecció de Dades.

  - Reial decret 156/1996, de 2 de febrer, pel qual es modifica l'Estatut de l'Agència Espanyola de Protecció de Dades.

  - Reial decret 1332/94, de 20 de juny, pel qual es desenvolupen alguns preceptes de la llei orgànica.

  - Reial decret 994/1999, d'11 de juny, pel qual s'aprova el Reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal.

  - Instrucció 1/1996, d'1 de març, de l'Agència de Protecció de Dades, sobre fitxers automatitzats establerts amb la finalitat de controlar l'accés als edificis.

  - Instrucció 1/1998, de 19 de gener, de l'Agència de Protecció de Dades, relativa a l'exercici dels drets d'accés, rectificació i cancel·lació.

  - Llei 59/2003, de 19 de desembre, de signatura electrònica.

– Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

- Autonòmica
  – Llei 8/2001, de 13 de juliol, de protecció de dades de caràcter personal a la Comunitat de Madrid.

  – Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades.

  – Llei 2/2004, de 25 de febrer, de fitxers de dades de caràcter personal de titularitat pública i de creació de l'Agència Basca de Protecció de Dades.

- Sanitària
  – Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.

  – Llei 14/1986, de 25 d'abril, general de sanitat.

  – Llei 16/2003, de 28 de març, de cohesió i qualitat del Sistema Nacional de Salut.

  – Llei 44/2003, de 21 de novembre, d'ordenació de les professions sanitàries.

  – Llei 25/1990, de 20 de desembre, del medicament.

  – Llei 35/1988, de 22 de novembre, sobre tècniques de reproducció assistida.

  – Llei 45/2003, de 21 de novembre, per la qual es modifica la Llei 35/1988, de 22 de novembre, sobre tècniques de reproducció assistida.

  – Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernents a la salut i l'autonomia del pacient, i la documentació clínica (Catalunya).

  – Llei 15/1998, de 9 de juliol, d'ordenació sanitària de Catalunya.

3.2. Una altra documentació d'interès

- Document de treball sobre el tractament de dades personals relatives a la salut en els historials mèdics electrònics (HME) - Grup de treball sobre protecció de dades de l'article 29.

- Conveni del Consell d'Europa sobre el respecte als drets humans i la biomedicina (1997).

- Recomanació 2/2004, de l'Agència de Dades de la Comunitat de Madrid sobre la custòdia, l'arxivament i la seguretat de les dades de caràcter personal de les històries clíniques no informatitzades.

3.3. Recursos a Internet

- Autoritats de control
  - Agència Espanyola de Protecció de Dades
    <www.agpd.es>

  - Agència Catalana de Protecció de Dades
    <www.apdcat.net>

  - Agència Basca de Protecció de Dades
    <www.avpd.euskadi.net>

  - Agència de Protecció de Dades de la Comunitat de Madrid
    <https://www.agpd.es/portalwebAGPD/ficheros_inscritos/
    titularidad_publica/indice_organismos/index-ides-idphp.php?
    organismo=QUdFTkNJQSBERSBQUk9URUNDSU9OIERFIERBVE9
    TIERFIExBIENPTVVOSURBRCBERSBNQURSSUQ=&tipo_admin=
    QURNT04uIFkgT1JHQU5JU01PUyBQ2kJMSUNPUyBERSBDLiBBVVRPT
    k9NQVM=&comunidad=Q09NVU5JREFEIERFIE1BRFJJRA==>

  - Comissió Nacional d'Informàtica i Llibertats - França
    <www.cnil.fr/index.php?aneu=5>

  - Information Comissioner's Office (ICO) - Regne Unit
    <www.ico.gov.uk/>

- Organismes europeus
  - Comissió Europea
    <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm>

  - Art.29 Data Protection Working Party
    <http://ec.europa.eu/justice_home/fsj/
    privacy/workinggroup/index_en.htm>

  - Unió Europea
    <http://europa.eu/index_es.htm>

  - Consell d'Europa

<http://hub.coe.int/>

- Universitats i docència
  - Universitat Catòlica de Lovaina, Centre Interdisciplinari d'Informàtica i Dret
    <http://www.law.kuleuven.be/icri/>

  - Universitat de Bolonya, Informàtica i Dret
    <http://www.cirsfid.unibo.it/cirsfid/index.html>

  - Universitat de Hannover, Institute for Legal Informatics
    <http://www.iri.uni-hannover.de/>

  - Universitat de Comillas, Institut d'Informàtica Jurídica
    <http://www.upcomillas.es/>

- Publicacions electròniques
  - Revista *Datos personales* (APD Comunitat de Madrid)
    <http://www.datospersonales.org/>

- Altres
  - Taller de criptografia de la Universitat de Granada
    <http://www.cripto.es/>

  - Associació Espanyola de Dret Sanitari
    <http://www.aeds.org/>