La protecció de dades d'una empresa de digitalització i l'encàrrec d'un fons fotogràfic corporatiu

TREBALL FINAL

Màster Oficial en Societat de la Informació i el Coneixement

Universitat Oberta de Catalunya

Alumna: Mercè Roselló Campdesuñer

Itinerari: *E-law i e-governmen*t (professionalitzador)

Director: Ricard Martínez Martínez

Juny 2011

SUMARI

1. Presentació i justificació

L'objectiu general d'aquest treball és presentar el projecte d'implementació d'un model de gestió de dades personals per part d'una empresa que ofereix serveis de digitalització, i amb l'encàrrec concret, procedent d'un fons fotogràfic corporatiu, de manera que pugui complir-se la legislació vigent. Per a fer-ho s'ha partit del supòsit pràctic simulat d'una PIME ubicada a Catalunya.

La protecció de les dades de caràcter personal en l'entorn de la Societat de la Informació i el Coneixement constitueix una àrea indispensable per a la seguretat de les empreses, indissociable de la necessària gestió de la informació i dels documents, i que no sempre ha estat prou coneguda o resolta en l'àmbit empresarial. A més d'aquesta necessitat, i atès que el sector de la digitalització a Catalunya és el d'un mercat encara no gaire consolidat d'acord amb el Pla elaborat per Doctodata (2008), l'empresa pretén trobar un nínxol per a la demanda, tot aprofitant la situació d'oferta limitada existent.

El motiu per a l'elecció de fons fotogràfics parteix, d'una banda, per les dades de caràcter personal, objecte d'estudi, que sovint contenen els fons de suport fotogràfic, i de l'altra, perquè, dins el sector de la digitalització a Catalunya, aquest tipus d'encàrrec especialitzat en fons de contingut cultural troba menys competidors que per als documents administratius (Doctodata, 2008). El poc interès per aquesta especialització es deu a què la digitalització de continguts culturals requereix habitualment una manipulació molt més complexa i personal més especialitzat, a més, de la probable dificultat de calcular els costos finals del procés.

Pel que fa a la procedència del fons, per tal d'aproximar-nos a la casuística d'encàrrecs que reben les empreses reals del sector a partir de la informació de l'informe diagnòstic elaborat per Doctodata (2008), el supòsit contempla el caràcter corporatiu del fons, atès que es tracta d'una opció força estesa. Així, si bé són coneguts els projectes de digitalització de fons públics i d'organitzacions del sector habitual, no és tan difosa o habitual la digitalització de fons procedents d'una persona física.

Quant al catàleg de serveis que s'ofereixen juntament amb el de digitalització, no està ben fixat, i cada comanda implica la negociació a la carta de les característiques tècniques del projecte. I per la mateixa raó de l'absència d'una d'oferta àmplia i variada de serveis, tampoc acostumen a estar ben definits ni els estàndards de qualitat ni els

procediments de treball. Per això, el servei de valor afegit d'aquest treball, pretén diferenciar-se, tot aportant una orientació al client en matèria de protecció de dades personals i preservació de documents.

A partir d'aquesta realitat, amb el present projecte es pretén observar el paper que ha de tenir una empresa de serveis de digitalització, d'una banda, en el tractament de les dades de caràcter personal i, de l'altra, respecte l'encàrrec que rep per digitalitzar i gestionar un fons fotogràfic de les característiques comentades. Totes elles, qüestions d'interès en l'àmbit disciplinari de la Documentació i, objecte d'estudi del Màster dins l'itinerari professionalitzador de Dret i Administració en Tecnologies de la Informació i la Comunicació (E-law i e-government), per manejar i aplicar els aspectes jurídics de tipus pràctic de la protecció de dades personals en aquest entorn social i tecnològic.

Abans d'iniciar l'exposició del treball, em cal agrair el suport i el temps finalment dedicat, del meu director del treball, Ricard Martínez Martínez, qui m'ha orientat en l'elecció del tema i en l'aclariment de conceptes jurídics nous en el context de l'itinerari del màster.

2. Metodologia i objectius del treball

El desenvolupament de la simulació d'aquest supòsit pràctic en l'entorn de l'itinerari professionalitzador d'E-law i e-government, ha tingut com a objectius principals els següents:

- Analitzar aspectes jurídics de cert grau de complexitat, a partir d'un exemple extret de la casuística del sector de la gestió documental en la Societat de la Informació i la Comunicació.
- Aportar solucions de síntesi i/o dades concloents del cas pràctic, que reflecteixin els coneixements apresos en el màster.
- Aportar la idea d'un servei de valor afegit, que completi la formació d'una reflexió entorn dels aspectes treballats.

Cal advertir que, per documentar el projecte de simulació, s'ha partit d'eines i recursos d'informació del sector públic i privat; tanmateix, qualsevol semblança que tinguin les dades del cas pràctic d'aquest treball amb la realitat, no ha estat cercada i és pura coincidència.

Aquest treball professionalitzador, a mode de projecte per a la implementació d'un model de gestió de les dades personals d'una empresa, s'estructura en set grans parts: en primer lloc, es parteix d'una visió global del marc legal i normatiu existent en matèria de protecció de dades, a escala autonòmica, estatal i comunitària; a continuació, s'ofereix una descripció de l'escenari de l'organització, amb les finalitats que persegueix, la seva infraestructura i els requeriments bàsics de compliment normatiu que necessita per prestar els serveis; un cop definit el concepte de fitxer jurídic, es passa a definir i aplicar els nivells de seguretat requerits segons la normativa per a cada fitxer, i es complementa la proposta amb una anàlisi de riscos de l'organització; posteriorment, s'exposen els principis de recollida d'acord amb la regulació i s'hi afegeixen altres principis vinculats, que procedeixen de la gestió documental; d'aquesta forma, s'arriba a abordar les fases de l'adopció de la normativa i que condueixen a l'aplicació de les mesures de seguretat per a cada fitxer tractat, unes mesures que es revisen per un procés de pre-auditoria; posteriorment, s'ofereix la descripció d'un servei de valor afegit, a mode d'informe del tractament realitzat i amb l'assessorament sol·licitat pel client entorn de la preservació i difusió de dades i de documents; i per finalitzar, s'ofereix una reflexió amb orientacions per a forjar la cultura organitzativa en la matèria i en el context de societat de la informació treballat al llarg del màster.

L'apartat més extens i, possiblement el més important del treball, integra tres fases d'adopció de la normativa: en primer lloc, els processos de creació i d'inscripció dels fitxers a l'Agència Espanyola de Protecció de Dades; en un segon lloc i, d'acord amb les dades subjectes a protecció, la informació i requeriments per al consentiment i la gestió dels drets d'accés, rectificació, cancel·lació i oposició; i una tercera fase, en relació amb les polítiques de seguretat, es tracta l'eina i el contingut del document intern de seguretat, s'explica la importància de les funcions del responsable que s'ha de fer càrrec de coordinar-lo i vetllar per al seu compliment, i es passa a determinar les mesures per a cada fitxer, tot comprovant que s'ajustin des de l'inici als requeriments d'un procés auditor.

A la part final d'aquest treball, i després del contingut exposat, es presenten, d'una banda, la relació de fonts consultades, agrupades per tipologies de recursos i documents i, d'altra banda, en annexos, les eines del cas pràctic, com poden ser, els fitxers notificats, el document de seguretat, alguns elements dels papers de treball per a l'auditoria, i altres detalls dels recursos emprats en els serveis prestats.

3. Marc teòric entorn de la protecció de dades:

El naixement de la societat de la informació als anys noranta, associada a la importància social, econòmica i cultural que adquireixen les tecnologies de la informació i les comunicacions, i ha estat tractada pel Reial Decret 1289/1999, de 23 de juliol, pel qual es crea la Comissió Interministerial de la Societat de la Informació i de les Noves Tecnologies. Segons la definició que fa aquest Reial Decret, en l'exposició prèvia a l'articulat:

> "La idea de **societat de la informació** engloba un conjunt d'activitats industrials i econòmiques, comportaments socials, actituds individuals i formes d'organització política i administrativa, d'importància creixent en les nacions situades en l'avantguarda econòmica i cultural, al que no poden sostreure els poders públics".

I afegeix sobre el paper de les tecnologies, que "la societat espanyola pot beneficiar-se d'aquesta transformació en la mesura que sigui capaç d'adoptar amb rapidesa certes **innovacions tecnològiques** i, en conseqüència, pugui gaudir de les noves oportunitats que s'ofereixen".

En aquest context, la informació es pot constituir coma a "valor de mercat", des del moment en què les aplicacions informàtiques permeten desenvolupar anàlisis qualitatives de les dades sobre un individu, que relacionades amb el conjunt d'informació disponible en les xarxes, donen un perfil de personalitat d'un subjecte (Martínez, 2005)

Per això, el tractament d'informació personal adquireix una importància fonamental, i davant la necessitat d'unes regles del joc que garanteixin els drets dels ciutadans, es recorre a l'ordenament jurídic perquè reguli l'ús de les tecnologies de la informació i les comunicacions. Part d'aquesta tasca ve regulada pel dret fonamental a la protecció de dades personals. I com veurem el desenvolupament normatiu per garantir la protecció de dades, va molt lligat no només a l'àmbit jurídic, sinó també a les possibilitats que permet i obre l'àmbit tecnològic.

A mida que Internet creix, hi sorgeixen problemes de tipus tecnològic, social i econòmic, que malgrat tots els intents de regulació per part de governs i institucions, no gaudeixen de consens, sinó de respostes per part de diverses comunitats limitades pel seu context institucional i la jurisdicció del seu context normatiu, que són grans perspectives de fragments dels problemes. Entenc que, de vegades, es produeix una "hibridació" (Berman, 2007) de drets, en un àmbit social, quan per exemple un

proveïdor recull dades a partir d'un formulari web. Així, no hi ha un codi universal de conducta establert per a la protecció de la privacitat de l'usuari. Però si un pluralisme de codis i algunes recomanacions fetes des de l'àmbit institucional a Internet. En qualsevol cas, amb independència de l'existència o no de codis de conducta corporatius, i de la inexistència d'un tractat internacional d'àmbit universal, la normativa de la Unió Europea està molt definida en matèria de protecció de dades.

D'altra banda, en la gestió de la protecció de dades personals d'una organització, i més concretament de dades personals sovint presents en els seus documents que també cal gestionar, com veurem d'acord amb Martínez (2005: mòdul 1), la legalitat vigent constitueix l'objectiu mínim a assolir, però, hi haurà casos en què els seus requeriments siguin superiors al mínim normatiu exigible. En tots ells caldrà garantir la compatibilitat entre el dret d'accés a la informació i documentació, i el dret a la protecció de les dades personals.

3.1. Legislació i drets fonamentals

La protecció de dades, com a conjunt de tècniques normatives o jurídiques, té per objecte garantir el dret fonamental consistent a què l'individu tingui la capacitat d'exercir un control real sobre la seva informació. Per tant, en la definició de la protecció de dades ens cal partir del concepte d'informació personal. Altres conceptes que s'hi relacionen i, que es troben a la legislació, són el dret a la **intimitat** i **vida privada**. (Martínez, 2005: m.1, 8).

L'objecte de protecció de dades abasta qualsevol tipus de dada personal, sigui o no íntima, el coneixement o ús del qual per tercers pugui afectar els seus drets. I a més afecta aquelles dades personals públiques, que pel fet ser accessibles al coneixement de qualsevol, no escapen al poder de disposició de l'afectat perquè així ho garanteix el dret a la protecció de dades. Per tant, el fet que les dades siguin de caràcter personal no significa que només tinguin protecció les relatives a la vida privada o íntima de la persona, sinó estan emparades totes aquelles dades que identifiquin o permetin la identificació de la persona, fins al punt de servir per a la confecció del seu perfil ideològic, racial, sexual, econòmic o de qualsevol altra característica, o per a qualsevol altra utilitat que en determinades circumstàncies constitueixi una amenaça per a l'individu.

D'acord amb el que assenyala pel Tribunal Constitucional en la sentència núm. 292/2000 serà dada de caràcter personal "qualsevol tipus d'informació personal, pública o privada". Aquesta és la sentència més rellevant, ja que remarca les qüestions relacionades amb la protecció jurídica de les dades personals i consolida de manera definitiva la consideració de la mateixa com un dret fonamental. Amb aquesta sentència, el Tribunal Constitucional consolida el dret fonamental a la protecció de dades, establert per l'art. 18.4 CE, segons el qual que integra:

> "un conjunt de drets subjectius, deures, procediments, institucions i regles objectives, per mitjà dels quals s'articula la tècnica de protecció de dades i exigeix el compliment d'una sèrie de principis, -qualitat de les dades, consentiment, secret, mesures de seguretat-, que garanteixin la seva efectivitat" (Martínez, 2005: m. 1, p. 9).

A continuació, s'exposa normatiu i jurídic bàsic que cal considerar, desenvolupat a Catalunya, a l'Estat Espanyol i a la Unió Europea en matèria de protecció de dades. Mirarem de fer referència també a alguns articles en relació amb el criteri de l'accés, tal i com recullen Rodríguez i Biescas (2010):

a) Espanya:

A l'Estat Espanyol, la Constitució Espanyola i la Llei del Patrimoni Històric Espanyol fan referència a la protecció de dades en abordar la qüestió de l'accés a la informació i als documents, mentre les altres lleis són específiques de la protecció de dades i els seus aspectes es veuran desenvolupats al llarg d'aquest treball.

- *Constitució espanyola 1978.*

El dret fonamental a la protecció de dades és un dret contemporani establert per l'art. 18 CE:

"**Article 18**

1. Es garanteix el dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.
3. Es garanteix el secret de les comunicacions i, especialment, de les postals, telegràfiques i telefòniques, excepte en cas de resolució judicial.
4. La llei limitarà l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets."

I especialment ens referirem a l'art. 20 de la CE sobre la llibertat d'expressió, i a comunicar o rebre informació per qualsevol mitjà, i en concret apartats 1 i 4:

o **Article 20**

"1. Es reconeixen i es protegeixen els drets:

a) A expressar i difondre lliurement els pensaments, les idees i les opinions mitjançant la paraula, l'escriptura o qualsevol altre mitjà de reproducció.

b) A la producció i a la creació literària, artística, científica i tècnica.

c) A la llibertat de càtedra.

d) A comunicar o a rebre lliurement informació veraç per qualsevol mitjà de difusió. La llei regularà el dret a la clàusula de consciència i al secret professional en l'exercici d'aquestes llibertats."

"4. Aquestes llibertats tenen el límit en el respecte als drets reconeguts en aquest títol, en els preceptes de les lleis que el desenvolupin i, especialment, en el dret a l'honor, a la intimitat, a la imatge pròpia i a la protecció de la joventut i de la infància."

I també, diu la llei regularà:

o **Article 105:**

"b) L'**accés** dels ciutadans als arxius i als registres administratius, **salvant el que afecti** la seguretat i la defensa de l'Estat, la indagació dels delictes i **la intimitat de les persones**."

- *Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.*

Segons el seu art. 1.3 "El dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge és irrenunciable, inalienable i imprescriptible". Tanmateix com diu en el seu art. 8.1 "No es regularà com a intrusió al dret l'honor, a la intimitat i a la imatge quan predomini un predomini un interès històric, científic o cultural rellevant". D'altra banda, l'article 8.2, regula el dret a la pròpia imatge.

- *Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD).*

Aquesta Llei orgànica, que s'aplica a tractaments automatitzats o no de dades personals, té com a objecte garantir i protegir, pel que fa al tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i la seva intimitat personal i familiar. També contempla l'àmbit d'actuació de l'entitat encarregada de vetllar pel compliment d'aquest dret, l'Agència Espanyola de Protecció de Dades i del Registre General de Protecció de Dades (Rodríguez; Biescas, 2010).

- *Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999 , de 13 de*

desembre de Protecció de Dades de caràcter personal, d'ara endavant RDLOPD.

Aquest Reial Decret desenvolupa aquells aspectes en què la seva norma superior (LOPD) que requereixen ser precisats i adaptats a la realitat més recent, per tal de fer front als riscos que per als drets de les persones poden suposar la recopilació i el tractament de les seves dades.

- *Llei 16/1985 Llei del Patrimoni Històric Espanyol (LPHE)*

"Art. 49.2 Forma part del Patrimoni Documental els documents de qualsevol època generats, conservats i reunits -o no en arxius i biblioteques- en el l'exercici de la seva funció per qualsevol organisme de caràcter públic, per les persones jurídiques -amb major capital de l'Estat- i per les persones privades, físiques o jurídiques, que gestionen de serveis públics.

Art. 49.3 També formen part els documents amb una antiguitat superior als 40 anys, generats, conservats o reunits en l'exercici de les seves activitats per entitats, fundacions i associacions de caràcter polític, sindical, religiós culturals i educatives de caràcter privat.

Art. 49.4 Així mateix, els documents amb una antiguitat superior als 100 anys generats, conservats o reunits per qualsevol altre entitat particular o persona física.

Art. 49.5 D'acord amb aquest article l'Administració de l'Estat pot declarar constitutius del Patrimoni documental aquells documents que sense arribar als 100 anys mereixin aquesta consideració.

Art. 52.3 Tots els propietaris de béns constitutius del Patrimoni Documental i Bibliogràfic han de permetre l'estudi per part dels investigadors, prèvia sol·licitud, sempre i quan això no suposi una intromissió dret a la intimitat personal i familiar i a la pròpia imatge dels particulars que podran negar-se la seva consulta."

Art. 57.1 Consulta dels documents del Patrimoni Documental

c) Els documents que contenen **dades personals** de caràcter policial, processal, clínic o que poden afectar a la seguretat de les persones, al seu honor, a la intimitat de la seva vida privada i familiar i a la seva imatge, no podran ser consultats sense el consentiment dels afectats o quan hagin passat **25 anys** de la seva **mort** del titular de les dades o **50 anys** de la **creació** del **document**, si no se'n coneix la data de la seva mort.

b) Catalunya:

La majoria de la legislació, es relaciona amb la protecció de dades, pel fet que en regula l'accés en aquestes.

- *Estatut d'autonomia de Catalunya (2006)*

Pel que fa a l'accés, especialment el seu article 31, referent al dret de totes les persones a "la protecció de les dades de caràcter personal contingudes en els

fitxers de la Generalitat, a accedir-hi, a examinar-les i a corregir-les". També es contempla l'accés i confidencialitat en matèria de salut en el seu article 23.3 i en matèria d'informació mediambiental en els art. 27.3 i 46.5.

- *Llei 9/1993 del patrimoni cultural català (LPCC)*

L'objectiu d'aquesta Llei és la protecció, la conservació, el creixement, la investigació, la difusió i el foment del patrimoni cultural català.

Art.19.2 S'entén per Patrimoni Documental:

Els documents produïts o rebuts, en l'exercici de llurs funcions i com a conseqüència de llur activitat política i administrativa, per la Generalitat, pels ens locals i per les entitats autònomes, les empreses públiques i les altres entitats que en depenen".

Els documents de més de 40 anys d'antiguitat produïts o rebuts, en l'exercici de llurs funcions, per persones jurídiques de caràcter privat que desenvolupen llur activitat a Catalunya".

Els documents de més de 100 anys d'antiguitat produïts o rebuts per qualsevol persona física i els documents de menys 100 que hagin estat produïts en suports de caducitat inferior als cent anys (...)".

Art. **30 Accés als béns culturals d'interès nacional**

Art. 30.1a) "Els propietaris, titulars d'altres drets reals i posseïdors de béns culturals d'interès nacional estan obligats a permetre l'examen i l'estudi dels béns pels **investigadors** reconeguts per alguna institució acadèmica, amb la presentació prèvia d'una sol·licitud raonada, avalada pel Departament de Cultura".

- *Llei 10/2001 d'arxius i documents (LAD).*

Distingeix entre documents públics i privats, que defineix en els capítols 6 i 7 respectivament. Crec que cal destacar els següents articles:

Art. 7.4 Les administracions i totes les entitats titulars de documents públics -i que els custodien- han de permetre l'accés i lliurar-ne una còpia o un certificat a les persones interessades garantint el dret a la intimitat personal (protecció de dades personals) i la reserva de d'aquelles dades protegides per lleis (exempcions).

Art. 14 Els propietaris de **documents privats** els poden dipositar **en un arxiu públic.** Si en l'acord de dipòsit no consta res en contra, l'arxiu pot:

b) "Facilitar la difusió dels documents amb finalitats culturals".

c) “Facilitar l’accés als documents en les condicions generals aplicables a la documentació pública”.

- *Llei 32/2010, de l’1 d’octubre, de l’Autoritat Catalana de Protecció de Dades.*

Llei que deroga la Llei 5/2002 de l’Agència Catalana de Protecció de Dades.

c) Unió Europea:

El naixement del dret fonamental a la protecció de dades s'inscriu en un corrent europeu de pensament jurídic, i també d'acció legislativa els punts culminants són l'article 18 de la Constitució Espanyola i l'art. 35 de la Constitució Portuguesa de 1975. En l'àmbit de la Unió Europea aquest dret s'inclou en el Projecte de Tractat, -fracassat, per cert- pel qual s'institueix una Constitució per a Europa i prové de l’article 8 de la Carta de Drets Fonamentals de la Unió Europea (2000). Aquesta norma en la praxi suposa una evolució del Conveni 108 del Consell d’Europa de 28 de gener de 1981, per a la protecció de les persones respecte al tractament automatitzat de dades de caràcter personal, ratificat per Espanya el 1984.

El bloc normatiu comunitari i internacional ha generat un conjunt de normes, principis i procediments que, amb diferents graus d'intensitat és comú a pràcticament tot Europa. (Martínez, 2005: 12-13).

La protecció de dades, a més de trobar-se recollida com a principi fonamental en diferents convenis, ha estat un dret específicament desenvolupat per la Directiva 95/46/CE del Parlament Europeu i del Consell de 24 de juliol 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. Aquesta norma estableix límits a la recollida i utilització de les dades personals i sol·licita la creació, a cada estat membre, d’un organisme nacional independent encarregat de la protecció de les dades (Rodríguez; Biescas, 2010). Igualment en aquest àmbit de la lliure circulació de les dades i al seu tractament, trobem el Reglament (CE) núm. 45/2001 d’aplicació a les institucions de la Unió Europea.

A més cal afegir la 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 o Directiva sobre la privacitat i les comunicacions electròniques i la Directiva 2006/24/CE, de 21 de febrer de 2006, del Parlament Europeu i del Consell sobre la conservació de dades tractades en relació amb la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions per la qual es modifica la Directiva 2002/58/CE.

A més de la Directiva 2002/58/CE, com assenyalen Rodríguez i Biescas (2010), en trobem d'altres que integren l'actual marc regulador de la UE de les xarxes i dels serveis electrònics per tal de garantir un nivell de protecció del dret a la intimitat pel que respecta al tractament de dades personals en el sector de les comunicacions electròniques: 2002/21/CE («Directiva marc»); 2002/20/CE («Directiva sobre autorització») i 2002/22/CE («Directiva sobre servei universal»), així com l'anterior directiva 97/66/CE.

Tanmateix, la Directiva 2009/136/CE modifica la Directiva 2002/22/CE, la Directiva 2002/58/CE i el Reglament (CE) 2006/2004 sobre la cooperació en matèria de protecció dels consumidors.

D'altra banda, l'accés a les dades es troba regulat fonamentalment per la *Carta de Drets Fonamentals de la UE* (2000) en el seu article 42, segons el qual "qualsevol ciutadà de la Unió o qualsevol persona física o jurídica que tingui el seu domicili social en un Estat membre té dret a accedir als documents del Parlament Europeu, del Consell i de la Comissió". I també ens parla de l'accés el *Tractat de la Unió Europea* (Tractat de Maastricht) (2002) en el seu article 1.3. (Rodríguez; Biescas, 2010).

3.2. Adaptació del marc jurídic al context tecnològic

L'origen del dret a la protecció de dades resideix en l'evolució de les tecnologies de la informació i de les comunicacions (TIC), i per tant, es tracta d'un dels anomenats *drets de tercera generació*. Aquests drets a més de l'àmbit de les TIC, també fan referència als àmbits cultural i mediambiental. Aquest fet obliga a conèixer amb detall el substrat material a què s'aplica la norma i per tant manejar els conceptes definits per la LOPD i pel RDLOPD. Per tant, no es tracta d'una pura aplicació

mecànica de la norma LOPD forçant, si cal, la realitat dels fets. Cal una comprensió de la realitat material sobre la qual s'aplica, així com un profund coneixement del sector jurídic sobre el qual s'aplica la Llei a causa del caràcter instrumental i/o transversal del dret fonamental a la protecció de dades. (Martínez, 2009a: 2)

En aquesta línia, a més de la legislació que es refereix estrictament a la protecció de dades, en el disseny d'un Servei de Digitalització que tracti gestió de documents i fons documentals caldrà contemplar-ne el marc jurídic específic, com les esmentades lleis del patrimoni i les dels arxius, en els àmbits català i espanyol. La regulació més recent dels serveis de la societat de la informació (SSI) es troba a la Directiva 2000/31/CE de 8 de juny de 2000, que fou objecte de transposició la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic. L'esmentada Directiva 2000/31/CE pren com a base la definició de SSI que en va fer la Directiva 98/34/CE del Parlament Europeu i del Consell, de 22 de juny de 1998, relativa a un procediment d'informació en matèria reglamentària relativa als serveis de la societat de la informació o Directiva de Transparència.

La definició legal dels "serveis de la societat de la informació" (SSI) es va establir a la Directiva 98/34/CE, concretament en l'article 1.2, que va resultar de la modificació de la Directiva 98/48/CE, referent a la protecció jurídica dels serveis d'accés condicional o basats en dit accés, on es recull: «tot servei prestat normalment amb remuneració, a distància, per via electrònica i a petició individual del destinatari serveis». (Peguera, 2006)

D'acord amb l'Annex de Definicions de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, el concepte de servei de la societat de la informació comprèn, en la mesura que constitueixin una activitat econòmica per al prestador de serveis: "la contractació de béns o serveis per via electrònica; la gestió de compres a la xarxa per grups de persones; la tramesa de comunicacions comercials, i el subministrament d'informació per via telemàtica". Els dos últims tipus de serveis seran tractats en aquest treball. Es contempla també el fet que, tant el "prestador de serveis", com els destinataris dels mateixos, poden ser persones físiques o jurídiques.

També entren dins la consideració de serveis a la societat de la informació en el mateix Annex, el "servei d'intermediació" concebut com aquell servei pel qual es facilita la prestació o utilització d'altres serveis de societat de la informació, com: "la

provisió de serveis d'accés a Internet, la transmissió de dades per xarxes de telecomunicacions, la realització de còpia temporal de les pàgines d'Internet sol·licitades pels usuaris, l'allotjament en els propis servidors de dades, aplicacions o serveis subministrats per altres i la provisió d'instruments de recerca, accés i recopilació de dades o d'enllaços a altres llocs d'Internet". Es tracta, per tant, d'un servei que no és aliè a un servei de digitalització, com veurem.

I en un entorn digital canviant i de regulació complexa, poden constituir un complement de gran ajut els manuals i directrius d'organismes i institucions sobre la seguretat i preservació de la informació, com l'Instituto Nacional de Tecnologías de Comunicación, o les guies adaptades a la ciutadania de les autoritats competents en la matèria.

3.3. Les normes ISO en gestió de documents

A banda del marc jurídic, les normes ISO que són estàndards tècnics, alguns dels quals certificables, però que a diferència de la major part de legislació, no són d'obligat compliment tret que ho requereixin alguns procediments institucionals, sinó que aporten unes pautes que, en sistematitzar processos, han de contribuir a facilitar l'acompliment de la regulació jurídica vigent.

En l'entorn digital canviant com en qualsevol altre entorn de treball, cal considerar els estàndards que ens permetin treballar en la millora contínua dels serveis. Així, els documents i evidències que constitueixen gran part del coneixement de tot tipus d'organitzacions, tenen com a funcions principals garantir-ne la seva conservació a llarg termini.

L'Organització Internacional de Normalització (ISO) és una federació mundial d'organismes nacionals, que en són membres. Des d'una perspectiva multidisciplinària, són diversos els Comitès Tècnics d'ISO que han assumit el repte de normalitzar els processos i tècniques aplicables a la gestió de documents i evidències electròniques.
En els darrers anys, s'han publicat una sèrie de textos normatius, traduïts per l'AEN/CTN 50 d'AENOR *Documentació* i adoptats com a Normes UNE. Vegem-ne els principals (Bustelo, 2008?):

- UNE-ISO 15489:2006 “Informació i Documentació: Gestió de documents”. Formada per dues parts, corresponents a generalitats i directrius, presenten bones pràctiques en gestió de documents en paper i electrònics.

- UNE-ISO 15836:2007 “Informació i Documentació: Conjunt d’elements de metadades Dublin Core”. Equivalent a la ISO 15836:2003 (IDT). Relacionada la Norma UNE-ISO 23081, presenta un nivell bàsic d’elements descriptius aplicables a qualsevol recurs electrònic.

- UNE-ISO 23081:2008 “Información y documentación: Procesos de gestión de documentos. Metadatos para la gestión de documentos”. Les dues parts d’aquesta norma fan palesa l’evolució UNE-ISO 15489:2006.

- UNE-ISO/TR 15801:2008 IN “Imagen electrónica. Información almacenada electrónicamente. Recomendaciones sobre veracidad y fiabilidad”. Equivalències amb: ISO/TR 15801:2004 (IDT)

  Amb solucions per garantir la fiabilitat de les imatges escanejades.

- UNE-ISO/TR 18492:2008 IN “Conservación a largo plazo de la información basada en documentos”. Equivalències amb: ISO/TR 18492:2005 (IDT).

- UNE-ISO/TR 26122:2008 IN “Información y documentación. Análisis del proceso de trabajo para la gestión de documentos”. Equivalències amb: ISO/TR 26122:2008 (IDT).

Existeixen també altres estàndards i recomanacions en matèria de seguretat a les xarxa. Cal destacar que, pròximament la norma ISO 30300 de gestió documental permetrà aglutinar en una única norma diversos aspectes transversals en l’eix estratègic d’un sistema organitzatiu: qualitat; medi ambient; seguretat de la informació; prevenció de riscos laborals; a més de gestió documental. D’aquesta forma, es podran veure els beneficis de treballar de forma integrada àrees, com la seguretat de la informació i la gestió documental que, com veurem es complementen.

4. L'organització: finalitats, recursos i requeriments normatius

En aquest apartat es fa una presentació de l'organització, del seu sistema d'informació i dels requeriments normatius bàsics per prestar els serveis. Els elements que s'hi exposen, de caràcter introductori, ens permetran posteriorment elaborar una anàlisi de riscos en diferents nivells de seguretat.

4.1. Visió, missió i objectius dels serveis

L'empresa FOTOSIC, SL, es composa per un equip interdisciplinari de professionals, que ofereix serveis de digitalització i gestió de documents corporatius, per a diferents tipus d'organitzacions. S'autodefineix per la següent visió i missió:

a) Visió

Esdevenir una empresa capdavantera en seguretat i qualitat documentals, especialitzada en serveis de digitalització i gestió de fons fotogràfics corporatius, mitjançant el compliment normatiu en el seu disseny dels requeriments bàsics en matèria de protecció de dades personals.

b) Missió: Proveir d'una gestió eficient de fons fotogràfics que pertanyin a persones identificables d'empreses i organitzacions, en el tractament per a la seva digitalització i publicació en línia, amb les garanties de compliment normatiu en matèria de protecció de dades.

c) FOTOSIC, SL ofereix serveis de digitalització -retoc segons els paràmetres del client-, gestió per al tractament de la imatge, indexació, classificació i integració en un servei d'allotjament Web, que el client farà seu com una Intranet. Els **objectius** d'aquest conjunt de servei de digitalització i gestió de fons que ofereix l'empresa són:

- Garantir una recerca d'informació més àgil.
- Proveir diversos usuaris, d'accés immediat i concurrent als mateixos documents, i estalviar còpies innecessàries.
- Reduir l'espai físic especialment en aquelles zones on és més costós.
- Estalviar temps i augmentar l'eficàcia en la gestió.
- Assegurar una estructura de seguretat per als usuaris que és alhora vàlida per protegir la informació.

- Preservar les fotografies originals, que es mantenen en els arxius, mentre es consulten les seves versions en suport digital.
- Confidencialitat i traçabilitat en la Gestió del Coneixement.
- Agilitat i eficàcia dels fluxos de treball.

4.2. Infraestructura: recursos humans, materials i logístics

4.2.1. Recursos humans:

Equip format per:

- Documentalista i pedagoga, directora del projecte i de l'empresa. Amb màster en Societat de la Informació i el Coneixement, especialitzada en dret de les Tecnologies de la Informació i les Comunicacions.
- Enginyer informàtic, especialitzat en temes de seguretat i en programes de digitalització.
- Arxivera, especialitzada en sistemes de gestió documental.
- Documentalista, especialitzada en tractament fotogràfic i en estudis de mercat.
- Administrativa-comptable, amb experiència comercial.

4.2.2. Recursos materials:

El servei disposa d'un equipament informàtic amb programari actualitzat i connexió a Internet, i ofereix un servei d'allotjament perquè els clients puguin accedir als documents escanejats. Per això, combina una infraestructura informàtica de client-servidor amb emmagatzematge en línia. Disposa també de gestió de documents, personalitzat a través del personal especialitzat, i d'acord amb les necessitats dels clients.

Servidors i emmagatzematge:

D'una banda, proveïdor d'Internet, com pot ser Telefònica, per tal d'oferir el servei de difusió a la web corporativa. Quant al servidor intern, consultable pel client, es cerca la millor solució, i no s'està lligat a una marca concreta. Així es pot contemplar algun servidor que permeti un rendiment a gran escala com el

PowerEdge de Dell. Una altra possibilitat són les que ofereix HP com: Sistemes de còpies de seguretat HP StorageWorks D2D o algun dels dispositius NAS.

També es treballa amb les còpies de seguretat en discs externs USB i es fa emmagatzematge en diversitat de suports.

Custòdia de documents i suports informàtics:

Tot i que els clients poden accedir als documents que es dipositen al Web, en opció d'Intranet, també es disposa d'armaris de seguretat ignífugs que garanteixen la custòdia dels suports informàtics propis i dels clients, i els protegeixen dels camps magnètics, dels danys electrostàtics i de la pols. El servei de recollida i trasllat es realitza per personal propi o per empreses de missatgeria.

Escàners, impressores i ordinadors:

Per començar es dota l'organització de dos escàners, dues impressores, quatre ordinadors, un portàtil i altres dispositius, amb les característiques que s'adjunten a l'*Annex 1*.

4.2.3. Recursos logístics:

Com a PIME i societat limitada, per les seves dimensions, ofereix un servei Outsourcing que es localitza en un únic pis a l'oficina de l'empresa.

Els serveis s'adreçaran principalment a empreses amb certa trajectòria, que puguin requerir les necessitats dels serveis, a persones i a institucions de qualsevol sector, i es difondran a través de la web corporativa. En aquest cas, caldrà contemplar els requeriments per contractar un servidor d'Internet, com veurem en els següents apartats.

Per obtenir finançament per als projectes de digitalització encomanats per entitats públiques o privades, s'hauran de presentar a concurs públic o obtenir un encàrrec directe. I per a la implementació de determinats projectes es pot cercar el suport de *partners* o socis, com Dell, Microgestió o Kodak.

Els recursos materials i humans del centre, hauran de permetre cobrir les següents fases d'un projecte documental: anàlisi del contingut, digitalització, post-indexació i classificació, integració en el catàleg corporatiu i desenvolupament sistemes documentals amb mètodes de preservació, accessibilitat i recuperació segurs en tot el procés.

Per això, es farà una formació prèvia i contínua del personal entorn de tota la normativa de seguretat i de qualitat. I per tal de garantir l'aplicació de la privacitat de les dades i de la seguretat, FotoSic signarà amb el client contractes de confidencialitat que compromet com diu la LOPD (art. 12.3) a no fer ús dels documents digitalitzats i a no guardar-ne cap còpia un cop finalitzada la prestació de serveis.

4.3. Requeriments bàsics de compliment normatiu per prestar els serveis

FotoSic, com a organització, ha contemplat els següents requeriments normatius en el disseny dels seus serveis i l'adquisició dels recursos necessaris per oferir-los.

4.3.1. Conceptes previs implicats en el servei

L'àmbit objectiu d'aplicació de la Reial Decret 1720/2007, de desplegament de la LOPD (RDLODP), ve definit en el seu article 1.1 com: "les dades de caràcter personal registrades en suport físic, que les faci susceptibles de tractament, i a qualsevol modalitat d'ús posterior d'aquestes dades pels sectors públic i privat." En la mateixa línia, estableix el Tribunal Constitucional en la STC núm. 292/2000 serà dada de caràcter personal qualsevol tipus d'informació personal, pública o privada. (Martínez, 2005).

Així mateix, l'article 2 de la RDLODP senyala *exclosos* del seu àmbit d'aplicació: tractaments de dades referides a **persones jurídiques** i fitxers que es limitin a incorporar les dades de les persones físiques que hi prestin els seus serveis- quan siguin consistents únicament en el nom i cognoms, les funcions o llocs exercits, l'adreça postal o electrònica, telèfon i fax professionals; dades relatives a empresaris individuals, quan hi facin referència en la seva qualitat de comerciants, industrials o naviliers; o persones mortes.

Aquest article és de primer ordre, per preveure dos fets que reprendrem en un apartat més avançat, entorn dels fitxers a tractar:

- Els fons corporatius queden exclosos de l'aplicació del RDLODP. En canvi, si aquests fons, en lloc de procedir d'una persona jurídica o d'un empresari individual, pertanyen a un client final, és a dir, a una persona física, sí que haurem d'aplicar el RDLODP.

- Pel que fa als fitxers que gestionin dades dels recursos humans de FOTOSIC, des del moment que requereixin més dades de les indicades en l'article 2, i la seva finalitat és diversa, ja que no és "contactar" sinó l'organització del personal, per exemple, per a la gestió de les seves nòmines, i sí quedaran acollits per aquesta normativa.

Segons l'article 5 del RDLODP, la **dada de caràcter personal** és: "qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables".

I amb relació a la persona identificable ens remetem a l'article 5 del RDLODP, "de la qual es pugui determinar, directament o indirectament, qualsevol informació referida a la identitat física, fisiològica, psíquica, econòmica, cultural o social". Però entenem que "una persona física no es considera identificable si la dita identificació requereix terminis o activitats desproporcionats". Així, sempre que qui hagi de realitzar el tractament tingui coneixement directe o indirecte a qui es refereix la imatge d'una fotografia o la identificació amb la IP d'un ordinador, tindrà la naturalesa de dada de caràcter personal i el tractament efectuat està sotmès a la normativa de protecció de dades (Martínez, 2005).

4.3.2. L'àmbit subjectiu d'aplicació de la LOPD

D'acord amb l'àmbit subjectiu d'aplicació de la LOPD, hem de distingir tres figures: el titular de les dades; el responsable del fitxer o tractament, i l'encarregat de tractament.

En primer lloc, el concepte de **titular de les dades** el trobem en la definició que fa l'article 5è del RDLODP, per **afectat** o **interessat**, com "la *persona física* titular de les dades que siguin objecte del tractament".

Cal tenir en compte que els titulars només podran ser persones físiques, en lògica coherència amb el que disposa l'art. 1 LOPD que remet el seu objecte de protecció als drets de les persones físiques (Martínez, 2005: m. 1). Per tant, aquells fitxers o tractaments que continguin dades únicament procedents de persones jurídiques quedaran exclosos de l'aplicació de la norma.

I pel que fa als empresaris individuals, tindrem en compte el que disposa l'article 2 del RDLODP, que n'exclou "quan hi facin referència en la seva qualitat de comerciants, industrials o naviliers". Tanmateix, en cas de dubte, la solució haurà d'adoptar-se en favor de la protecció dels drets individuals (Martínez, 2005).

Quant al **responsable dels seus fitxers o tractament,** segons la definició del RDLODP és "la persona física o jurídica, de naturalesa pública o privada", qui decidirà, sola o juntament amb altres, "sobre la finalitat, contingut i ús del tractament, encara que no ho realitzi materialment"; i també "els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats".

Per tant, el responsable del fitxer o tractament sempre és aquell qui decideix sobre l'ús de les dades personals i en l'àmbit privat, com el de FOTOSIC, el responsable sempre correspon amb el titular de l'activitat (Martínez, 2005). FOTOSIC serà responsable dels seus propis fitxers, com per exemple, els qui afectin a temes del seu personal, o els dels seus proveïdors.

Els serveis que es presten a d'altres organitzacions són un tipus d'activitat que, en l'àmbit de la protecció de dades, s'atribueixen a la figura de **l'encarregat del tractament** definit en l'article 5, paràgraf i, del RDLOPD com:

> "la persona física o jurídica, pública o privada, o òrgan administratiu que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del tractament o del responsable del fitxer, com a conseqüència de l'existència d'una relació jurídica que l'hi vincula i delimita l'àmbit de la seva actuació per a la prestació d'un servei.
>
> També poden ser encarregats del tractament els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats".

Així, FOTOSIC, com a encarregada de tractament, serà la persona jurídica i privada que tractarà dades per compte del responsable del fitxer, és a dir, del client propietari del fons, a través d'un contracte.

D'acord amb l'article 12 de la LODP, cal una clàusula dins d'aquest contracte de serveis que signin la consultant amb els seus clients, que contempli el següent:

- Que **l'encarregat del tractament només ha de tractar les dades d'acord amb les instruccions del responsable del tractament** i que no les pot aplicar ni utilitzar amb una finalitat diferent de la que figuri en el contracte esmentat, ni comunicar-les a altres persones, ni tan sols per conservar-les.
- El contracte també ha d'estipular les mesures de seguretat a què es refereix l'article 9 d'aquesta Llei que l'encarregat del tractament està obligat a implementar.
- Una vegada complerta la prestació contractual, les dades de caràcter personal i suports o documents que les continguin, han de ser destruïdes o tornades al responsable del tractament.
- Si l'encarregat del tractament destini les dades a una altra finalitat, les comuniqui o les utilitzi incomplint les estipulacions del contracte, també ha de ser considerat responsable del tractament i ha de respondre de les infraccions comeses.

I la possibilitat de subcontractació de serveis amb un tercer per part de l'encarregat de tractament –per ex. un servidor d'Internet o el servei de neteja-, es regirà per les condicions establertes a l'article 21 del Reial Decret 1720/2007. La primera d'elles és que el responsable del fitxer, li hagi encomanat o l'hagi autoritzat a fer-ho, sempre a nom i per compte del mateix responsable.

Tanmateix, no caldrà autorització quan: s'especifiquin els serveis i l'empresa en el contracte o l'encarregat en comuniqui, al responsable, les dades que identifiquin l'empresa abans de la subcontractació; el tractament per part del subcontractista s'ajusti a les instruccions del responsable del fitxer; l'encarregat i l'empresa subcontractista formalitzi el contracte i aquesta sigui considerada encarregada del tractament. I la tercera condició, és que si es fa necessari

subcontractar una part de servei que no s'ha previst en el contracte, aquesta part s'ha de sotmetre al responsable del tractament en els aspectes esmentats.

4.3.3. El tractament de les dades i els seus components:

El **tractament de les dades** personals, es farà des del primer moment de recepció i preparació per a la digitalització de la documentació, que segons l'art. 5 t) de la RDLOPD consisteix en:

> "qualsevol operació o procediment tècnic, ja sigui **automatitzat o no**, que permeti la recollida, gravació, conservació, elaboració, modificació, consulta, utilització, modificació, cancel·lació, bloqueig o supressió, així com les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències."

Els conceptes vinculats amb aquest procediment són:

Sistema d'informació: "conjunt de fitxers, tractaments, programes, suports i, si s'escau, equips utilitzats per al tractament de dades de caràcter personal." (RDLOPD, art. 5)

En primer lloc, es fa necessari aportar la idea de *sistema d'informació* que és un referent de primer ordre en el procés d'inscripció i d'adopció de mesures de seguretat, nou respecte de la LODP, i que pot resultar més entenedor que el concepte de 'fitxer' quan escau aplicar en la praxi les previsions normatives.

Mentre en aquesta definició, es fa referència als fitxers lògics, que poden ser fitxers informàtics, en el procés d'inscripció es produeix el que podem anomenar d'una manera una mica artificiosa una "inscripció de fitxers jurídics" que no hem de confondre (Martínez, 2009b). Per tant, el conjunt de fitxers lògics –programari, fulls de càlcul, llistats d'una base de dades ...- que utilitza el responsable per treballar un únic àmbit funcional, com pot ser la gestió de nòmines, integraran el fitxer jurídic d'aquell àmbit.

A continuació s'inclouen altres conceptes que apareixen en la definició:

Fitxers: "qualsevol conjunt organitzat de dades de caràcter personal que permeti l'accés a les dades d'acord amb uns criteris determinats, sigui quina sigui la forma o modalitat de la seva creació, emmagatzematge, organització i accés". (RDLOPD, art. 5).

I l'article diferencia com atenent a la seva titularitat, els fitxers poden ser públics o privats –com en el cas d'aquest treball- i en funció del seu tractament poden ser automatitzats o no.

Per tant, el fitxer jurídic pot estar integrat per fitxers automatitzats i/o per fitxers manuals o no automatitzats –com podrien ser les nòmines o factures en suport paper. En cas que contingui ambdós tipus de fitxers, en el procés d'inscripció, farem constar que es tracta d'un fitxer mixt.

Suport:
Es tracta d'un "objecte físic que emmagatzema o conté dades o documents, o objecte susceptible de ser tractat en un sistema d'informació i sobre el qual es poden gravar i recuperar dades. ". (RDLOPD, art. 5. ñ)

Per la seva possibilitat de transport de dades, el concepte de suport –com Pen-Drives, DVDs, CDs – comporta que haurem de preveure un seguit de mesures de seguretat en l'apartat corresponent.

I d'acord l'article 5 (n) del RDLOPD, el **sistema de tractament** és la "manera en què s'organitza o utilitza un sistema d'informació" i existeixen sistemes d'informació automatitzats, no automatitzats o parcialment automatitzats. En el cas que ens ocupa, es tractarà d'un tractament en bona part automatitzat.

5. Nivells de seguretat requerits i anàlisi de riscos

Per dissenyar les mesures de seguretat més adequades, cal conèixer prèviament els riscos i vulnerabilitats de tipus tècnic i organitzatiu en el tractament dels fitxers, atès que la seguretat no pot consistir en una aplicació mecànica dels criteris normatius (Martínez, 2009b). Amb aquest objectiu, es pretén obtenir una visió de conjunt per a l'establiment de polítiques de seguretat, que contempli, d'una banda, els nivells de seguretat del RDLOPD d'acord amb el tipus de dades i finalitats d'ús, i de l'altra una anàlisi que permeti avaluar els riscos de l'organització.

Els continguts d'aquest apartat s'exposen en quatre etapes: en primer lloc, una descripció dels nivells de seguretat segons la norma; en segon lloc, s'aplicaran els nivells als fitxers objecte de tractament i s'il·lustraran amb exemples; en tercer, es farà

una anàlisi global de les vulnerabilitats i fortaleses en seguretat de la PIME, que permeti orientar la política en seguretat; i, finalment, s'enumeraran alguns riscos a contemplar en l'adopció de mesures de seguretat addicionals per la normativa, i amb referència a possibles encàrrecs que rebi FOTOSIC, SL.

5.1. Nivells de seguretat segons la norma

El RDLODP en el seu article 80 identifica tres nivells de mesures de seguretat aplicables als fitxers que continguin dades de caràcter personal: bàsic, mitjà i alt. L'establiment d'un o altre nivell de seguretat s'adopta en funció de la diferent sensibilitat de les dades personals incloses en els arxius.

Les mesures que ha d'adoptar l'empresa per tal de garantir la seguretat de les dades personals, d'acord amb el Títol VIII del RDLODP, es fixen en funció del nivell de seguretat corresponent al fitxer, i en funció del suport del mateix (automatitzat o no automatitzat).

Els nivells de seguretat són acumulatius, de forma que per exemple, els fitxers de nivell alt han de complir les mesures previstes per als fitxers de nivell alt, mitjà i bàsic.

D'acord amb l'article 81 del RDLODP, s'ha d'aplicar cada nivell de seguretat en els fitxers o tractaments que continguin les següents dades personals:

o Nivell bàsic:

Qualsevol dada que no sigui nivell mitjà o alt. Així, podem entendre, per exemple: nom, cognoms, dades de contacte (adreça, telèfon, correu-e ...)

o Nivell mitjà

• Dades relatives a la comissió d'infraccions administratives o penals

• Dades regides per l'article 29 de la LODP referent a la prestació de serveis d'informació sobre solvència patrimonial i crèdit.

• Dades que ofereixin una definició de les característiques o personalitat dels ciutadans i permetin avaluar aspectes de la seva personalitat o comportament.

• Dades de les quals siguin responsables i es relacionin amb les seves finalitats, de:

- Les administracions tributàries
- Les entitats financeres

- Les entitats gestores i serveis comuns i les mútues d'accidents de treball i malalties professionals de la Seguretat Social.
- Els operadors que prestin serveis de comunicacions electròniques

o Nivell alt

Ideologia; afiliació sindical; religió i creences; origen racial; salut i vida sexual; dades recollides per a finalitats policials sense consentiment de les persones afectades; dades derivats d'actes de violència de gènere.

Tanmateix, el tractament no serà lineal, i haurem de recordar, per exemple, les excepcions previstes per al nivell alt, a l'apartat 5è de l'article, quan no tinguin relació amb la finalitat del tractament i no siguin persones identificables, i de 6è, o en el cas que es demani una dada de salut com a deure públic. En aquests casos, les dades es tractaran com a nivell bàsic.

5.2. Nivells de seguretat dels fitxers a tractar

El primer encàrrec que rep FotoSic procedeix del fons de la **Fundació arquitectes amb l'habitatge digne**, i consisteix en la digitalització d'un fons fotogràfic de la història de la Fundació creada el 1985, per a la difusió i foment de les seves activitats. Com s'ha vist en l'apartat de requeriments tècnics, aquest encàrrec correspon al d'una persona jurídica, no és de l'àmbit d'aplicació del RDLODP.

Tanmateix, per tal que tinguem en compte els nivells de seguretat del seu fons a l'hora de fer la digitalització i gestió per a la difusió dels seu fons, l'empresa ens passa un quadre dels nivells de seguretat que ha aplicat al seu fons i que es comenta en l'apartat del servei d'encàrrec al final d'aquest treball.

Pel que fa a la qüestió central dels fitxers propis de FOTOSIC, per tal de determinar quines mesures de seguretat caldrà aplicar segons la normativa, en primer lloc hem de detectar el nivell de seguretat aplicable als fitxers i tractaments de dades de caràcter personal.

FOTOSIC és responsable de dos fitxers jurídics: un de *Gestió de personal i nòmines*, i l'altre de *Gestió de clients i/o proveïdors*. S'han analitzat els seus usos i finalitats de les dades, per a determinar-ne el nivell exigible, de la forma següent:

- Gestió de personal i nòmines:

La finalitat del primer fitxer és gestionar les dades dels recursos humans que integren l'equip per a la confecció de nòmines i cobraments, l'arxiu i gestió dels seus currículums que han estat necessaris en el procés de selecció, i per incloure en la sol·licitud d'algun projecte públic, així com la gestió d'altres currículums i informes de les entrevistes que, per al procés de selecció, van ser contrastats amb dades dels seus perfils a LinkedIn, amb el seu consentiment, i algunes dades personals necessàries en matèria de prevenció de riscos.

En aquesta última matèria, en qualsevol cas, com que el servei de prevenció de riscos el porta una mútua externa, és aquesta qui tracta dades de salut, i únicament en el cas que fos necessària una adaptació del lloc de treball es podrien inferir de FOTOSIC, que no coneix directament dades de salut, i únicament rep algunes sessions d'ergonomia i de simulacres d'emergència. Per tant, tot aplicant les possibilitats de segregar fitxers, la mútua externa, n'aplicarà el nivell alt, mentre FOTOSIC, només n'haurà d'aplicar el bàsic en relació amb aquest tema.

En principi, d'acord amb les finalitats del fitxer, n'hi hauria prou en aplicar-hi el nivell bàsic, però es fa necessari aplicar-hi un **nivell mitjà de seguretat**, atès que els currículums contrastats amb pàgines impreses del LinkedIn que es continuen conservant, contenen dades referents a aficions, amistats, entramat de relacions i activitat a les xarxes socials, és a dir, "característiques de la personalitat o que permeten avaluar-ne determinats aspectes", d'acord amb l'article 81.2 del RDLODP. Per tant, com que l'empresa, considera important contractar empleats amb certes habilitats socials i això imposa accedir a aquestes dades i aplicar un nivell mitjà de seguretat.

- Gestió de clients i/o proveïdors:

En el segon fitxer, hi ha les dades de contacte de la Fundació, però també hi ha dades de clients, que són persones físiques, de vegades familiars hereus d'un fons, per la qual cosa es fa necessari aplicar la normativa.

La finalitat i usos previstos en aquest fitxer són la gestió comptable, fiscal i administrativa entorn dels clients, així com la publicitat i prospecció comercial. L'empresa envia publicitat als clients que no s'hi oposen i elabora un perfil de les seves preferències a partir de la informació que rep de les pàgines a Facebook o de pàgines web corporatives. En el seu contingut trobem entre altres, dades

referents a les circumstàncies socials, a finances, informació comercial i a característiques personals que permeten avaluar-ne el seu comportament com a usuaris o clients finals, i que ens porten a aplicar també el nivell mitjà.

Les dades personals de cada fitxer estan detallades als annexos 2 i 3 de notificacions i al document de seguretat, annex 5.

5.3. Anàlisi global de seguretat DAFO

Un cop establerts els nivells de seguretat que determinaran les mesures que volem aplicar, ara ens cal analitzar els recursos que disposa l'organització en matèria de seguretat, fet que ens permetrà acabar de dotar dels elements necessaris que requereixi el disseny de la seva política de seguretat. Com ens trobem a l'inici de la implantació, aquesta anàlisi pretén ser una previsió bastant exhaustiva de possibles vulnerabilitats i amenaces, així com de les fortaleses i avantatges per fer-los front.

Aquests riscos externs i interns, juntament amb l'observació de punts forts interns i oportunitats externes amb què poder-los fer front, ens permetran procedir a una anàlisi DAFO (Debilitats, Amenaces, Fortaleses i Oportunitats) en diferents àmbits o tipus d'actuació (Martínez, 2009), de FOTOSIC, sigui com a encarregada de tractament, però també com a responsable dels seus fitxers.

	PUNTS FORTS	**PUNTS FEBLES**
INTERN: FotoSic (inclou a tercers que treballin amb les dades internes)	**De tipus físic:** • Gaudir de còpies de seguretat **De tipus informàtic i documental:** • Una infraestructura tècnica adequada, amb els sistemes i suports més adients • Pla de manteniment i substitució dels components del sistema • La transferència periòdica de les dades a nous suports. • Assegurar les condicions apropiades de emmagatzematge i tractament de suports **De tipus personal:** • L'assignació de la responsabilitat individual –en el cas dels comentaris en blocs, repartida amb l'usuari, autor dels comentaris – amb els beneficis associats en les condicions de treball i la qualitat de la informació. • Formació en la cultura organitzativa de la protecció de dades.	**De tipus físic:** • Precarietat de l'original difícil de restaurar **De tipus informàtic i documental:** • Generació 'natural' d'errors (equip informàtic). • Risc d'avaries del suport o del servidor • Pèrdua de l'accés, en cas de fallida comercial • El risc que quedin fitxers temporals, un cop finalitzat el servei per l'encarregat*. • Problemes per a l'eliminació correcte d'altres fitxers que cal destruir. • Risc en la integritat del fitxer en la transferència de dades d'un sistema o suport a un altre; • Risc sobre l'autenticitat dades en fet d'afegir o actualitzar metadades.

	• Deure de secret exigible segons l'article 10 LOPD2, a tots els que intervinguin en el tractament de les dades.	**De tipus personal:** • Risc d'actes del personal per inadvertència (p.e. desconnectar l'electricitat, llençar suports o perdre'ls…)
	OPORTUNITATS	**AMENACES**
EXTERN: INTERNAUTES I FACTORS DE L'ENTORN	**De tipus físic:** • Plans de prevenció de catàstrofes. **De tipus informàtic i documental:** • Controls de seguretat del sistema periòdics avalats per la normativa • L'eficàcia en el disseny del sistema de gestió del fons, ha de permetre beneficiar-se d'una consulta pública àgil, tot respectant els originals, les dades personals i el dret d'accés al fons per part dels ciutadans. **De tipus personal:** • Amb ajut de les normes ISO, adaptació a la legislació vigent (LOPD) que permet regular el sistema de gestió de les dades. • Empara de la llei, o en cas de comentaris difamatoris, dels jutjats i tribunals segons la llei • Comunicació del pla estratègic que asseguri la confiança als clients potencials	**De tipus físic:** • Catàstrofes naturals (p. e. incendis o inundacions) • En la recollida o recepció del material original, risc a ser malmès en el transport, a pèrdua o sostracció. • Altres amenaces que pesen sobre l'autenticitat (UNESCO, 2003) definida per la integritat i/o la identitat dels fitxers. **De tipus informàtic i documental:** • *Malware* o atacs informàtics malintencionats • Danys incidentals causats per altres atacs no dirigits al sistema • Robatori d'informació personal, com ara noms d'usuari i contrasenyes. **De tipus personal:** • Suplantació de la identitat de l'usuari • Per part d'usuaris als social media, comentaris difamatoris, que infringeixin algun dret de la pàgina, o que atemptin contra l'honor, la pròpia imatge i la intimitat personal

Com s'observa, els diferents tipus d'amenaces i debilitats poden afectar les dades emmagatzemades, sigui en la integritat de bona part d'ells, en la identitat i fins i tot en el seu accés (UNESCO, 2003: 123-124).

5.4. Riscos que ha de tenir en compte l'encarregat en l'adopció de mesures

Com s'ha dit, FOTOSIC és una empresa que es dedica al tractament de fitxers dels seus clients. En els encàrrecs que s'escaigui aplicar els requeriments bàsics de la normativa, segons l'article 12 de la LODP, entre el responsable del fitxer i l'encarregat del tractament s'haurà d'establir un contracte. El paper de l'encarregat del tractament i el seu estatut es troba desenvolupat en el capítol tercer del títol II i l'article 82 de la RDLODP, que exigeix que el reconeixement de les circumstàncies

concretes en què es realitzi la prestació de l'encarregat es faci constar en el document de seguretat, així com el nivell de seguretat que determinarà les obligacions que aquest haurà d'assumir.

D'acord amb aquests requeriments, la tasca de l'encarregat no consistirà en detectar els riscos, sinó en fer que es pugui confiar en la seva organització i adopti les mesures necessàries per evitar-los. Anem a enumerar el conjunt de riscos que haurà de contemplar FOTOSIC i que li comportaran l'adopció mesures d'acord amb el que hagi establert en cada encàrrec:

a) Riscos en l'entrada i sortida de dades

En primer lloc, en el procés de recollida d'originals, que la Fundació vol fer arribar a FotoSic, existeixen riscos de sostracció o pèrdua d'informació o l'accés indegut a aquesta durant el seu transport. També s'entén per sortida de documents i suports "els compresos i/o annexos a un correu electrònic, i tots aquells fora dels locals sota el control del responsable del fitxer o tractament". Per tant, com veurem, la sortida l'ha d'autoritzar el responsable del fitxer o ha d'estar degudament autoritzada en el document de seguretat, segons l'article 92 del RDLODP sobre mesures de nivell bàsic.

b) Riscos en l'accés remot

En segon lloc, caldrà atendre les responsabilitats sobre els riscos per part de l'encarregat, pel fet que la digitalització i tractament es realitzarà en els locals de l'encarregat, i durant el procés, les dades amb accés remot i simple accés en mode consulta a les dades, s'emmagatzemaran en el servidor i suports propis. Per tant, d'una banda, igual com per als seus fitxers, haurà de controlar el risc de *malware* i d'atacs malintencionats, així com el funcionament correcte dels dispositius; i de l'altra s'haurà d'assegurar d'esborrar per complet el fitxer del client en finalitzar el contracte, com estipula la normativa.

c) Riscos en el sistema d'informació de l'encarregat

D'acord amb l'apartat sisè de l'article 88 del Reglament del (RDLODP), com que les dades personals del fitxer del responsable es tracten de manera exclusiva en el sistema de l'encarregat, el responsable ho anotarà en el seu document de seguretat. L'encarregat haurà de seguir les mesures del Reglament i les instruccions del responsable del fitxer entorn del local i sistema on es realitza el tractament.

d) Riscos associats al treball fora dels locals del responsable del fitxer

D'altra banda, pel que fa als riscos associats al treball fora dels locals del responsable del fitxer o encarregat del tractament, segons l'article 86 del Reglament, existeix la possibilitat d'autorització prèvia segons la qual l'accés es pot «establir per a un usuari o per a un perfil d'usuaris i determinant un període de validesa per a les mateixes». I el responsable també pot delegar autoritzacions per acostar el procés de presa de decisions als gestors més propers als sistemes d'informació, en cas, per exemple de retoc o restauració d'una fotografia malmesa.

e) Riscos de buidat inadequat

Finalment, també són susceptibles de posar en risc els sistemes d'informació, les pràctiques de buidat inadequat de suports o l'accés a documents pendents de ser eliminats i no sotmesos a custòdia. Aquest risc s'haurà d'abordar per contracte i en els corresponents documents de seguretat segons l'article 83 del RDLOPD, com desenvoluparem en els següents apartats sobre les mesures de seguretat.

Caldrà contemplar aquests riscos, en les mesures addicionals quan constitueixi un requeriment, i d'altres de semblants d'acord amb els que es derivin dels fitxers que FOTOSIC té com a responsable, i que s'han assenyalat anteriorment.

6. Principis de qualitat de les dades i algunes qüestions a considerar

D'acord amb l'article 8 del RDLOPD, FOTOSIC com a responsable del seus fitxers, haurà de partir d'uns principis previs a la recollida i tractament de les dades de caràcter personal, que es concretaran en els següents objectius:

- Tractar les dades de **manera lleial i lícita**, garantint així els drets de les persones segons els quals aquestes han de ser protegides des de la seva obtenció i ús fins a la finalització del seu tractament.
- Recollir les dades amb **finalitats determinades, explícites i legítimes**. Això comporta, d'una banda, que les dades objecte de tractament no es poden fer servir per a finalitats incompatibles amb aquelles per a les quals les dades han estat recollides, i de l'altra que han de ser adequades, pertinents i no excessives en relació amb les esmentades finalitats.

• Aconseguir dades **exactes i mantenir-les actualitzades**, de manera que responguin amb veracitat a la situació actual del seu titular. Es consideren exactes les dades que faciliti directament de l'interessat.

• **Conservar les dades personals només durant el temps necessari** per a les finalitats del tractament per al qual han estat recollides, i cancel·lar-les quan hagin deixat de ser necessàries o pertinents per al fi amb què es van obtenir.

I la LOPD en el seu títol II referent als principis de la protecció de dades, juntament amb els principis de qualitat, inclou el deure de secret en el seu article 10:

> "El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional pel que fa a les dades i al deure de guardar-les, obligacions que subsisteixen fins i tot després de finalitzar les seves relacions amb el titular del fitxer o, si s'escau, amb el seu responsable."

D'altra banda, es fa necessari comentar un altre valor important que haurà de tenir els serveis de FOTOSIC: l'autenticitat de les dades.

6.1. Qüestions documentals prèvies: la importància de l'autenticitat

Un altre aspecte important a valorar amb conseqüències en el tractament de les dades personals, i que recollíem en l'anàlisi de riscos, fa referència a l'**autenticitat** d'aquestes, els riscos de la qual segons la UNESCO (2003), fan referència a dos aspectes:

- Aquells que pesen sobre la *identitat,* i no permeten distingir un objecte d'un altre, cosa que es pot deure a confusions en la identificació de les dades, a canvis dels identificadors o a la manca de documentació sobre les relacions entre les diferents versions o còpies.

- O sobre la *integritat*, com la majoria de canvis de continguts, que es deuen a les amenaces que pesen sobre les dades que conformen l'objecte.

Aquests riscos que, com veurem més endavant haurem de tenir presents en les mesures del tractament automatitzat dels fitxers –per exemple, en la identificació i autenticació d'usuaris- són traslladables també als documents en suport físic.

Tot seguint, de forma orientativa, la *Guia* que la Direcció General de Patrimoni Cultural (2010) ha elaborat per als projectes de digitalització de la Xarxa d'Arxius Comarcals que s'encarreguen a empreses i professionals especialitzats, tot i que FotoSic no serà qui determinarà els paràmetres per digitalitzar el fons, s'hauran de fer unes consideracions sobre alguns dels riscos amb els quals es pot trobar en la

seva tasca entorn de la integritat i la identitat dels fitxers objecte del seu tractament, i que escauen també per als seus propis fitxers. Així haurà de contemplar diversos aspectes com l'estat físic amb què arribin els documents, per tal de poder-ne valorar el seu grau de manipulació.

7. Fases d'adopció de la normativa

En aquest apartat es descriuen les fases del procés d'implantació de la normativa en protecció de dades. En una primera fase, s'aborda la identificació dels fitxers jurídics que cal inscriure a l' Agencia Española de Protección de Datos. En una segona fase, es revisen les dades precisen el consentiment dels interessats, i es tracta el dret a informar, així com la gestió dels drets d'accés, rectificació, cancel·lació i oposició. Finalment, la tercera fase, permet concretar a partir de l'elaboració del document de seguretat, el seu responsable i les mesures que cal aplicar segons el nivell exigible per a cada tipus de fitxer.

7.1. Creació i adaptació de fitxers

D'acord amb la necessitat de notificar els fitxers al Registre de l'Agencia Española de Protección de Datos, establerta en la normativa, en primer lloc, l'empresa ha d'identificar les dades de caràcter personal que s'estan manejant en el seu àmbit i com es troben organitzades. En aquest subapartat, es farà una revisió de les obligacions que determina la LODP en matèria de notificació de fitxers, i després d'identificar els fitxers creats per FOTOSIC, s'exposaran aspectes a considerar en el procés d'inscripció a l'AEPD.

A. <u>Descripció breu de les obligacions en aquesta matèria</u>

El client pel qual fem l'encàrrec és una persona jurídica que, com hem dit, per l'article 2 del RDLODP, no s'acull a la norma, el fitxer de FOTOSIC. No obstant això, el fitxer que integra les seves dades personals, n'integra totes les dels clients, entre ells persones físiques, per la qual cosa escau notificar l'esmentat fitxer de gestió de clients en els termes del RDLODP.

L'obligació legal de notificació dels fitxers a l'Agència de Protecció de Dades, per tal que siguin inscrits pel Registre General, és prèvia a la creació de fitxers i ve regulada per l'art. 26 de la LOPD. En el cas de fitxers existents aquesta cal fer-la amb la major brevetat possible. Si en el termini d'un mes, l'Agència de Protecció de

Dades no ha emès resolució sobre la sol·licitud, s'entén inscrit el fitxer automatitzat amb caràcter general.

Per a la notificació i inscripció de fitxers, caldrà seguir l'establert al capítol II del Títol cinquè de la RDLODP que amplia el contingut de la LODP. Així d'acord amb l'article 55, en el seu apartat 2n, com a fitxers de titularitat privada, han d'indicar un seguit d'elements que els identifiquen, com el responsable, les seves finalitats i usos, el col·lectiu de persones sobre el qual s'obtenen les dades, el nivell de mesures de seguretat exigible, entre altres. També, diu l'article, que si s'escau, cal identificar l'encarregat del tractament on estigui ubicat el fitxer i els destinataris de cessions i transferències internacionals de dades.

Atès que en moltes ocasions FOTOSIC actuarà com a encarregada del tractament, escau subratllar que en aquests casos l'obligació d'inscripció del fitxer a tractar pertany al responsable, que haurà d'incloure en el seu cas l'existència d'un encarregat.

Tanmateix, la responsabilitat de FOTOSIC rau en els fitxers propis que genera, com els llistats amb dades del personal i de l'empresa client. Per tant, per al desenvolupament de la seva tasca, FOTOSIC haurà de notificar els seus fitxers propis que continguin dades personals.

La notificació es farà per a cadascun dels fitxers jurídics. Això, pot suposar que cadascun d'aquests estigui compost al mateix temps per fitxers automatitzats i no automatitzats, tal i com contempla l'article 56 de la RDLODP:

> "Quan les dades de caràcter personal objecte d'un tractament estiguin emmagatzemades en diferents suports, automatitzats i no automatitzats o hi hagi una còpia en suport no automatitzat d'un fitxer automatitzat, només cal una sola notificació, referida al fitxer esmentat".

Un exemple el trobarem en el fitxer de personal de FOTOSIC, que es troba integrat per documents en suport paper i documents en línia, és a dir, que es tracta d'un fitxer mixt.

Pel que fa a la notificació per a la modificació i supressió de fitxers, ve regulada per l'article 58 del RDLODP, i també competeix a FotoSic com a responsable del fitxer, qui ha de vetllar per la seva inscripció actualitzada i per la notificació de supressió,

per cancel·lar-ne la seva inscripció a registre. En el formulari de notificació, s'han de complimentar no només les dades modificades de notificacions prèvies, sinó totes, atès que es tracta d'una notificació substitutiva de l'anterior. Les disposicions que s'han d'indicar són les mateixes que per a la creació de fitxers, regulades per l'art. 20.2 LOPD.

Pel que fa a la supressió, en les disposicions que es dictin, segons l'art. 20.3 de la LOPD, cal destacar que "se n'ha d'establir el destí o, si s'escau, les previsions que s'adoptin per destruir-los".

B. Recerca de fitxers

El pas previ a la inscripció a l'AEPD, correspon a la identificació correcta dels fitxers. Recordem la definició de fitxer aportada per l'article 5 del RDLODP, segons la qual, per observar si les dades personals estan organitzades en fitxers, cal reflexionar sobre el tipus de dades personals que fa servir, i analitzar si aquestes dades són emmagatzemades de forma organitzada, i que el seu accés es faci d'acord amb uns criteris determinats. A més, com comentàvem en l'apartat de requeriments d'aquest treball, un fitxer jurídic pot incloure una àmplia diversitat de documents i suports, sempre que afectin s'utilitzin per a les finalitats d'un mateix àmbit de gestió.

Aquest procés, s'ha revisat i ha contemplat dos aspectes:

a) *Tècnic, de verificació dels PC's i arxius no automatitzats*.

Comprovació de fitxers i registres que contenen els ordinadors, així com dels fitxers existents en suport paper -fase per a la qual s'han utilitzat els programes de treball d'un programa d'Auditoria, fixats per a cada nivell (Dobaño) (vegeu l'Annex 6).

b) *Indagació, d'Auditoria amb els usuaris.*

Per tal d'acabar de verificar l'existència dels fitxers, s'ha aplicat als usuaris un qüestionari de cada nivell, en funció de les funcions i permisos que tinguin assignades, (adjunts a l'Annex 6). També es realitza un altre qüestionari a la Directora- gerent.

En el procés de comprovació, s'ha verificat l'existència dels següents fitxers:

1. *Gestió de personal i nòmines* (fitxers automatitzats i no automatitzats)
Inclou documentació i programari en matèria de recursos humans: gestió de nòmines, currículums, formació de personal, prestacions socials, control horari, promoció, selecció i prevenció de riscos, entre altres.

De nivell mitjà, d'acord amb el comentat en l'apartat anterior sobre l'art. 81.2 RDLODP.

2. *Gestió de clients i proveïdors* (fitxer automatitzat)
Es tracta de la gestió econòmica, comptable, de facturació, fiscal, administrativa, de cobraments i pagaments entorn de clients i proveïdors de l'empresa. Inclou documents relatius a processos d'auditories i serveis relacionats, com consultories. D'altra banda, també conté documents referents a publicitat i prospecció comercial.

Així, per exemple, per la seva vinculació amb els temes de clients, en aquest fitxer s'inclouen els documents de revisió que controla el/la responsable de seguretat, com gestió d'entrada i sortida de suports, les autoritzacions, el control d'incidències, així com tots aquells documents útils de cara a l'Auditoria externa.

D'altra banda, si bé tots els documents que s'utilitzen per a la 'Gestió d'usuaris i d'accessos al sistema', es podrien desar en el fitxer de gestió de personal, però es troben dins aquest fitxer, amb vistes a que es puguin donar d'alta usuaris, que no formin part del personal del centre, com determinats proveïdors.

També, de nivell mitjà, d'acord amb el comentat en l'apartat anterior sobre l'art. 81.2 RDLODP.

C. <u>Procés d'inscripció amb l'explicatiu NOTA</u>
El procediment d'inscripció per a la notificació de fitxers de titularitat pública inclou els elements esmentats a l'article 55 del RDLODP, que corresponen a camps dels formularis electrònics de l'AEPD. L'inici del procediment de creació, modificació o supressió de fitxers es farà d'acord amb l'art. 130 del Títol IX de la RDLODP.

Veiem un exemple de procediment de notificació. Per a fer-ho es descarregarà del web de l'Agència, el formulari interactiu NOTA en format PDF que permet la

presentació de notificacions a través d'Internet amb i sense certificat de signatura electrònica.

En primer lloc, se'ns demanarà:

- El tipus de sol·licitud d'inscripció: entre les opcions alta, modificació o supressió, cliquem l'opció d'**alta** de fitxer.
- Model de la declaració: per als fitxers destinats a la gestió de clients, existeix un **formulari tipus**, pel qual optarem.
- Forma de presentació: que pot ser amb certificat digital de signatura electrònica o sense. En aquest segon cas, es pot fer a través d'Internet amb presentació convencional del Full de sol·licitud, per imprimir-lo, signar-lo manualment i entregar-lo a l'Agència, o bé, mitjançant formulari en suport paper amb codi de barres bidimensional PDF 417 que cal remetre físicament a l'Agència. Per tal de mostrar totes les etapes per Internet, utilitzarem la segona opció, amb presentació de la sol·licitud convencional.

  Els annexos 2 i 3 corresponen als formularis omplerts dels fitxers notificats.

  Veiem un exemple del procés de notificació:

NOTIFICACIÓ DE *GESTIÓ DE CLIENTS I/O PROVEÏDORS*

a. Dades del responsable del fitxer

Denominació social del responsable del fitxer: FOTOSIC

Activitat: N35: COMERCIO I SERVICIOS ELECTRÓNICOS

I la resta de dades sobre la localització de l'establiment del responsable, que en aquest cas es trobarà en una localitat de la mateixa província de Barcelona.

a. Drets d'oposició, accés, rectificació i cancel·lació

Una carta a l'adreça postal Avda. de la Clota, 12, 5è 7a de Barcelona (08135) o bé un correu electrònic a l' adreça electrònica següent, des d'un compte de correu prèviament notificat pel titular per garantir que l'exercici del dret sigui personalíssim: arco@fotosic.com

b. Dades de l'encarregat del tractament

En aquest cas, per aquests fitxers, no n'hi ha.

c. Identificació i finalitat del fitxer

Com hem clicat l'opció de formulari tipus per al fitxer amb nom que fa referència a clients i/o proveïdors, la descripció de finalitat ens surt per defecte la de Gestió de clients i/o proveïdors. Hi afegim: Publicitat i prospecció comercial.

d. Origen i procedència de les dades

Ens sortirà per defecte i correspondrà a l'interessat o al seu representant legal, tot entenent per col·lectius o categories d'interessats: clients i usuaris, proveïdors i persones de contacte.

e. Tipus de dades, estructura i organització

Aquí se senyalen les dades personals que contingui la base de dades de clients / proveïdors. Per això es revisarà les que surten per defecte, i en el seu cas s'afegiran els aspectes específics de l'organització, com la signatura electrònica, a dades de caràcter identificatiu.

f. Mesures de seguretat exigides

D'acord amb el que s'ha argumentat, indiquem nivell mitjà.

g. Cessió o comunicació de dades

Les categories que es mostren corresponen als destinataris de cessions que apareixen per defecte en un fitxer tipus com el triat. No s'ha previst la difusió d'aquestes dades en espais referents a FotoSic, a través d'empreses de publicitat. En cas que així, fos caldria marcar també les empreses dedicades a publicitat o MK directe.

Posteriorment abans de signar, s'omplirà el full de sol·licitud corresponent, amb les dades de la persona física que actuï en representació del responsable del fitxer davant l'AEPD, i una adreça postal a efectes de notificació.

7.2. Dades subjectes a la normativa

Veiem en aquesta fase, el tipus de principis i obligacions previstes en la normativa en matèria de dades de caràcter personal, a què estan subjectes les dades que recull l'empresa.

Recordem que, la persona jurídica és una de les excepcions de l'àmbit d'aplicació de la norma, d'acord amb l'article 2 del RDLODP. Així, pel que fa fitxer notificat 'Gestió de clients i/o proveïdors' cal diferenciar entre aquells clients que tenen la condició de persona jurídica empresari o professional, i els que tinguin la condició de persona física. Els primers són una excepció de l'àmbit d'aplicació de la norma, segons l'article 2 del RDLODP. En canvi, els segons entren dins l'aplicació de la normativa, per la qual cosa, en cas que ens trobéssim davant d'un client d'aquest tipus, hauríem d'aplicar el que preveu sobre el seu tractament, el Capítol II del RDLODP.

Tanmateix, haurem de contemplar altres requeriments de la prestació de serveis de FotoSic que es defineixen com a *serveis de la societat de la informació*, d'acord amb la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI). Recordem que entre aquests serveis, FotoSic inclou: d'una banda, serveis d'intermediació com la transmissió de dades per xarxes de telecomunicacions, l'allotjament en els propis servidors de dades, i la provisió d'instruments d'accés a les dades; de l'altra, la tramesa de comunicacions comercials i el subministrament d'informació per via telemàtica.

A continuació comentem els efectes que tenen aquests requeriments, en el dret d'informar als clients, i com ho contemplarem en l'A*vís legal* (Annex 4).

7.2.1. Informació i requeriments de consentiment

Les dades de caràcter personal dels recursos humans de FotoSic quedaran exemptes necessitat de consentiment d'acord amb l'article 10, apartat 3 b) del RDLODP, perquè les sol·licita el responsable del tractament en ocasió de la subscripció d'un contracte o precontracte o de l'existència d'una relació laboral de la qual n'és part l'afectat i les dades són necessàries per al seu compliment.

Tampoc caldrà el consentiment, pel que fa al fitxer notificat de *Gestió de clients i/o proveïdors*, quan hi hagi una "subscripció d'un contracte o precontracte o de l'existència d'una relació negocial (…) de la qual sigui part l'afectat i siguin necessaris per al seu manteniment o compliment", com recull el mateix article i apartat del RDLODP.

I per a la disposició de dades personals de clients a tercers, com servidors o xarxes socials, tampoc serà necessari el consentiment en els termes de la llei, mentre hi hagi relació contractual, d'acord amb l'article 11 de la LODP. d'acord amb l'apartat c de l'article: "Quan el tractament respongui a l'acceptació d'una relació jurídica per a la qual calgui necessàriament la connexió del tractament esmentat amb fitxers de tercers, i la comunicació només és legítima quan es limiti a la finalitat que la justifiqui, i aquesta finalitat es pugui verificar." I tampoc, si l'usuari ja figura en "fonts accessibles al públic", com el Facebook, segons l'apartat b de l'article.

Així doncs, en el moment que el client signi el nostre contracte de prestació de serveis –en suport paper-, li adjuntarem l'avís legal de l'Annex 4.

FotoSic, com a prestadora de serveis d'allotjament de dades i d'acord amb l'article 16 de la LSSI, no és responsable de la informació emmagatzemada a petició del destinatari, sempre que: "a) No tinguin coneixement efectiu que l'activitat o la informació emmagatzemada és il·lícita o que lesiona béns o drets d'un tercer susceptibles d'indemnització, o b) Si en tenen, actuïn amb diligència per retirar les dades o fer impossible accedir-hi (…)".

Com s'observa en el mateix avís legal, les comunicacions comercials per via electrònica requeriran el consentiment del destinatari, en els termes establerts pels articles 19 al 22 de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI). La sol·licitud de consentiment s'haurà d'efectuar abans de finalitzar el procediment de contractació i el destinatari podrà revocar-ne en qualsevol moment el consentiment prestat amb la simple notificació de la seva voluntat al remitent.

Així mateix, FotoSic habilitarà un procediment senzill i gratuït perquè els destinataris de serveis puguin revocar el consentiment que hagin prestat, amb informació accessible per mitjans electrònics sobre els esmentats procediments, i que vindrà inclosa en la mateixa comunicació electrònica:

Si vol deixar de rebre les nostres comunicacions publicitàries i promocionals, si us plau cliqui en el següent enllaç.

7.2.2. Gestió dels drets ARCO

Quan respecte dels fitxers per als quals sigui d'aplicació el RDLODP, com el cas dels clients finals o del personal, l'afectat vulgui exercir els seus drets d'accés, rectificació, cancel·lació o oposició, ha de formular la sol·licitud d'aquests drets directament o a través d'una persona que acrediti actuar en representació d'aquell, atès que són personalíssims d'acord amb l'article 23 del RDLOPD.

També tindrem en compte les condicions generals per a l'exercici d'aquests drets, segons l'article 24 del mateix Reial Decret:

> "1. Els drets d'accés, rectificació, cancel·lació i oposició són drets independents, de tal manera que no es pot entendre que l'exercici de cap d'aquests drets és un requisit previ per a l'exercici dels altres.
> 2. S'ha de concedir a l'interessat un mitjà senzill i gratuït per a l'exercici dels drets d'accés, rectificació, cancel·lació i oposició.
> 3. L'exercici per part de l'afectat dels seus drets d'accés, rectificació, cancel·lació i oposició és gratuït i en cap cas pot suposar un ingrés addicional per al responsable del tractament davant el qual s'exerceixen."

En l'aspecte pràctic dels fitxers de FOTOSIC, s'adjunten a l'Avís legal referenciat, l'opció d'enviament a un Apartat de Correus amb sobre prefranquejat, en el cas dels fitxers mixtes, i l'opció vàlida en tots els fitxers automatitzats, d'una adreça de correu electrònic.

a) Dret d'accés

Aquest dret proporciona al titular de les dades el dret de conèixer quines dades té el responsable del fitxer o tractament sobre la seva persona. Així, l'interessat pot sol·licitar i obtenir informació de les seves dades de caràcter personal sotmeses a tractament, i de l'origen de les dades.

D'acord amb l'article 29 del RDLODP, el responsable del fitxer, disposi o no de dades de caràcter personal dels afectats, ha de resoldre sobre la sol·licitud d'accés en el termini màxim d'un mes a comptar del moment de la seva recepció. I si en el transcurs d'aquest termini no ha respost la petició d'accés, l'interessat pot interposar la reclamació que preveu l'article 18 de la Llei

orgànica 15/1999, de 13 de desembre. En cas d'estimar la sol·licitud, l'accés s'ha de fer efectiu en el termini dels deu dies següents a la notificació i la resposta al dret d'accés s'ha de fer utilitzant qualsevol mitjà que acrediti l'enviament i la recepció d'aquesta.

Igualment, el responsable del fitxer o tractament pot denegar-ne l'accés, acord amb l'article 30, quan el dret ja s'ha exercit en els dotze mesos anteriors a la sol·licitud, llevat que s'acrediti un interès legítim a aquest efecte.

b) Rectificació

Consisteix en el dret de l'afectat per tal que es modifiquin les dades que siguin inexactes o incompletes (art. 31.1 RDLOPD), cosa que suposa la correcció i actualització de les seves dades. Tal i com indica l'article 32 del RDLODP, la seva sol·licitud "ha d'indicar a quines dades es refereix i la correcció que s'ha de fer, i ha d'anar acompanyada de la documentació justificativa del que se sol·licita". Disposi o no de dades personals dels afectats, el responsable del fitxer o tractament, haurà d'atendre el dret de rectificació en el termini de deu dies naturals, i per a fer-ho utilitzar-ne qualsevol mitjà que acrediti l'enviament i la recepció. Si transcorregut el termini no n'obté resposta, l'interessat pot interposar la reclamació que preveu l'article 18 de la Llei orgànica 15/1999, de 13 de desembre. En cas que les dades rectificades haguessin estat cedides prèviament a un tercer -per ex. una xarxa social -, el responsable del fitxer té l'obligació de notificar al cessionari la rectificació practicada, en el mateix termini.

Com en el cas dels drets de cancel·lació (art. 33 RDLODP), es podran denegar: en els supòsits en què ho prevegi una llei o una norma de dret comunitari aplicable directament o quan aquesta llei o norma impedeixin al responsable del tractament revelar als afectats el tractament de les dades a què es refereixi l'accés".

En qualsevol cas, el responsable del fitxer ha d'informar l'afectat del seu dret a demanar la tutela de l'Agència Espanyola de Protecció de Dades o, si s'escau, de les autoritats de control de les comunitats autònomes, conforme al que disposa l'article 18 de la Llei orgànica 15/1999, de 13 de desembre.

c) Cancel·lació

D'acord amb l'article 31.2 del RDLODP, aquest dret faculta l'interessat a què se suprimeixin les dades personals que siguin inadequades o excessives, sense perjudici del deure de bloqueig conforme a aquest Reglament. En qualsevol cas, s'han de cancel·lar quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual foren registrades.

Tal i com indica l'article 32 del RDLODP, en la sol·licitud de cancel·lació, l'afectat ha d'indicar a quines dades es refereix, així com aportar a aquest efecte la documentació que ho justifiqui, si s'escau. El responsable del fitxer o tractament, disposi o no de dades personals de l'afectat, haurà d'atendre la sol·licitud del dret de cancel·lació en el termini de deu dies naturals, i per a fer-ho utilitzar-ne qualsevol mitjà que acrediti l'enviament i la recepció. Si transcorregut el termini no n'obté resposta, l'interessat pot interposar la reclamació que preveu l'article 18 de la Llei orgànica 15/1999, de 13 de desembre. En cas que les dades cancel·lades haguessin estat cedides prèviament a un tercer -per ex. una xarxa social -, el responsable del fitxer té l'obligació de notificar en el mateix termini al cessionari la cancel·lació practicada.

I finalment, segons l'article 33 del RDLODP, no hi haurà cancel·lació quan s'hagin de conservar les dades de caràcter personal o, si s'escau, les relacions contractuals entre la persona o l'entitat responsable del tractament i l'interessat que van justificar el tractament de les dades. Els supòsits i procediments de denegació dels drets, seran els mateixos que per als drets de rectificació.

Tanmateix, la cancel·lació, que d'acord amb la definició del RDLODP, consisteix en "el procediment en virtut del qual el responsable cessa en l'ús de les dades", implica el bloqueig de les dades, per tal d'impedir-ne el tractament excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per a l'atenció de les possibles responsabilitats nascudes del tractament, per si hi hagués cap incompliment de la LOPD, i només durant el termini de prescripció de les responsabilitats, que és de tres anys d'acord amb la LOPD. Un cop transcorregut aquest període, s'han de suprimir les dades.

No obstant això, per al cas de les dades referents al personal, aquest període serà de quatre que és el termini de prescripció de les obligacions fiscals a la llei de l'IRPF -Llei 35/2006, de 28 de novembre, de l'Impost sobre la Renda de les Persones Físiques i de modificació parcial de les lleis dels Imposts sobre Societats, sobre la Renda de no Residents i sobre el Patrimoni.

d) Oposició

Dret que suposa la facultat d'oposar-se al tractament de les dades que li concerneixen, perquè no es porti a terme, o cessi en els supòsits següents recollits per l'article 34 (RDLODP):

> "a) Quan no sigui necessari el seu consentiment per al tractament, a conseqüència que hi hagi un motiu legítim i fundat, referit a la seva situació personal concreta, que ho justifiqui, sempre que una llei no disposi el contrari.
> b) Quan es tracti de fitxers que tinguin per finalitat la realització d'activitats de publicitat i prospecció comercial, en els termes que preveu l'article 51 d'aquest Reglament, sigui quina sigui l'empresa responsable de la seva creació.
> c) Quan el tractament tingui per finalitat l'adopció d'una decisió referida a l'afectat i basada únicament en un tractament automatitzat de les seves dades de caràcter personal, en els termes que preveu l'article 36 d'aquest Reglament."

Quan la sol·licitud al responsable del fitxer, es faci basant-se en la lletra a) de l'article anterior, s'hi han de fer constar els motius fundats i legítims, relatius a una situació personal concreta de l'afectat.

Com en els casos anteriors, el responsable del fitxer o tractament, disposi o no de dades personals dels afectats, haurà d'atendre el dret de rectificació en el termini de deu dies naturals, i per a fer-ho utilitzar-ne qualsevol mitjà que acrediti l'enviament i la recepció. Si transcorregut el termini no n'obté resposta, l'interessat pot interposar la reclamació que preveu l'article 18 de la Llei orgànica 15/1999, de 13 de desembre. Així mateix, caldrà excloure del tractament les dades relatives a l'afectat que exerceixi el seu dret d'oposició o denegar motivadament la seva sol·licitud en el mateix termini de deu dies.

Així mateix, haurem de considerar l'article 36, del RDLODP, sobre el dret d'oposició referit a les decisions basades únicament en un tractament automatitzat de dades. Els interessats tenen dret d'exercir-lo, quan la decisió amb efectes jurídics o significatius es basi únicament en un tractament

automatitzat de dades, per avaluar determinats aspectes de la seva personalitat, com ara el seu rendiment laboral, crèdit, fiabilitat o conducta. Tanmateix, els afectats poden quedar sotmesos a una d'aquestes decisions, quan: s'hagi adoptat en el marc de la subscripció o execució d'un contracte a petició de l'interessat, sempre que se li atorgui la possibilitat d'al·legar el que estimi pertinent; o l'autoritzi una norma amb rang de llei que estableixi mesures que garanteixin l'interès legítim de l'interessat.

D'acord amb l'article 14 del RDLODP, es facilitarà un mitjà senzill i gratuït si vol oposar-se al tractament, com els exposats a l'*Avís legal*. Si hi ha constància que la comunicació s'ha retornat, no es podrà fer el tractament.

7.3. Aplicar les polítiques de seguretat

Després de les fase d'adaptació dels fitxers i de la fase d'obligacions de tractament i de recollida de dades - el dret d'informar, els requeriments del consentiment i la gestió de drets ARCO-, es procedeix a l'adopció de les mesures de caràcter tècnic, organitzatiu i jurídic que estableix la LODP i el RDLODP, per tal de garantir la seguretat de les dades personals. Entre aquestes mesures s'inclou l'elaboració del document de seguretat que descriu les dades emmagatzemades, les mesures de seguretat adoptades i les persones que tenen accés a aquestes dades.

El document de seguretat és un deure regulat pel Capítol II del RD 720/2007 i constitueix una eina útil per treballar la política de seguretat de l'empresa, transmetre-la als usuaris involucrats en el seu sistema d'informació, i evidenciar-ne el grau d'adopció per part de l'organització. Passem a definir-lo i concretar-lo.

7.3.1. Document de seguretat

D'acord amb l'article 88 del RDLODP, el document de seguretat ha de recollir les mesures tècniques i organitzatives d'obligat compliment per al personal amb accés als sistemes d'informació que contenen o han d'incorporar dades de caràcter personal. I, com afegeix el mateix article, es tracta d'un document de caràcter intern de l'organització que s'ha de mantenir actualitzat en tot moment.

Atès que el document de seguretat pot ser únic, en el cas de FOTOSIC n'hi ha un de sol que inclou tots els fitxers o tractaments. El nostre document conté els aspectes mínims previstos per l'esmentat article i recollits pel model de

document elaborat l'AEPD: àmbit d'aplicació del document i recursos protegits; mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit en aquest Reglament; funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers; estructura dels fitxers i dels sistemes d'informació que els tracten; procediment de notificació, gestió i resposta davant les incidències; procediments de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats; mesures que sigui necessari adoptar per al transport de suports i documents, i per a la destrucció dels documents i suports o, si s'escau, la reutilització d'aquests últims.

I quan s'han d'incloure mesures a partir del nivell mitjà, com és el cas del fitxers objecte de tractament, a més dels aspectes mínims, d'acord amb el RDLODP s'han d'afegir aquests altres aspectes, que hem contemplat al document de seguretat: identificació dels responsables de seguretat, i controls periòdics que s'hagin de realitzar per verificar el compliment del que disposa el mateix document.

El document de seguretat de FotoSic s'ha elaborat segons el model guia de l'Agència Espanyola de Protecció de Dades, i s'ha revisat amb les proves descrites en el Paper de Treball PT -1.1 del programa d'Auditoria (Velasco Dobaño, 2005).

A la següent taula es mostren els requisits mínims que es demanen en el procés d'auditoria per al nivell mitjà de seguretat previst, d'acord amb la regulació més recent de l'article 88 del RDLODP, així com la relació dels mateixos amb els apartats en el Document de Seguretat (*vegeu* Annex 5):

REQUISITS MÍNIMS AUDITORIA	*VIST*	*APARTAT DOCUMENT SEGURETAT*
1. Àmbit d'aplicació del document amb especificació detallada dels recursos protegits*	__/__/__	1 i 4; Annex I (a i b) i IX
2. Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit en aquest Reglament.		2 i Annexos I, III, IV, VIII
3. Funcions i obligacions del personal.		3 i Annex IV I X
4. Estructura dels fitxers.		Annex I (a i b)
5. Descripció dels sistemes de tractament.		Annex I (a i b)
6. Procediment de notificació, gestió i resposta d'incidències.		4 i Annex VI
7. Procediments de realització de còpies de seguretat.		2, Annex I (a i b) i Annex III
8. Procediment de recuperació de dades en els fitxers o tractaments automatitzats.		4 i Annex III
9. Identificació del Responsable de Seguretat.		2 i 3, i Annex I i II
10. Procediment dels controls periòdics.		5 i Annex XI
11. Mesures per a la destrucció de suports i documents, o si s'escau, la reutilització de suports.		2 i Annex V
12. Mesures per al transport de suports i documents.		2 i Annex III i VIII

* Per recursos protegits entenem, fitxers que contenen dades de caràcter personal que es troben sota la responsabilitat de l'empresa, incloent-hi els sistemes d'informació, suports i equips utilitzats per al tractament de dades de caràcter personal, que hagin de ser protegits (art. 88 del RDLODP).

7.3.2. Informació i obligacions del personal

D'acord amb l'article 89 del RDLODP, en el document de seguretat s'han definit les funcions i obligacions de cadascun dels usuaris o perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació, així com també les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament.

També, s'hi ha previst que la comunicació al personal de la normativa continguda en el document de seguretat, la faci arribar el responsable de seguretat, amb un comprovant signat que n'asseguri la seva recepció.

En les revisions caldrà valorar que les funcions del personal descrites en el document de seguretat concordin i siguin coherents amb l'organigrama funcional (Velasco Dobaño, 2005). Així, com també analitzar el llistat actualitzat de personal –incloses les responsables de seguretat- i el llistat actualitzat d'usuaris del sistema, per comprovar que aquests són coherents amb les funcions detallades en el document de seguretat.

Com diu Martínez (2009b), la seguretat no és responsabilitat d'una única persona ja que sovint es requereixen de diverses persones al càrrec dels sistemes d'informació, o de l'especialització del personal amb analistes, programadors, gestors d'aplicacions, gestors de xarxes, entre altres. Per això, l'article 84 del RDLODP contempla la possibilitat de delegar les autoritzacions del responsable del fitxer i incorporar-les al document de seguretat on han de constar les persones habilitades per atorgar aquestes autoritzacions, així com aquelles en les quals recau aquesta delegació.

7.3.2.1. Responsable de seguretat

Com s'ha dit, l'obligació de designar un responsable de seguretat està definida per als tractaments de fitxers de nivell mitjà i alt (Guia LOPD). Per tant, s'ha contemplat respecte dels fitxers de FotoSic de nivell mitjà.

Atès que segons l'article 95 del RDLODP, en el document de seguretat, es poden assignar un o diversos responsables de seguretat que s'ocupin de coordinar i controlar les mesures definides, i que aquesta designació pot ser diferenciada per a cada fitxer o tractament, s'ha optat per aquesta opció tal i com es constata al document de seguretat. El motiu ha estat per tal que d'ajustar la posició del perfil funcional de cadascun dins l'organigrama de l'empresa, al correcte desenvolupament de les seves funcions, tal i com preveuen els papers de treball d'Auditoria (Velasco Dobaño, 2005), tot i que es tracta d'un càrrec rotatiu.

En el procés de selecció, l'empresa ha considerat que les funcions de responsable de Seguretat, han de ser les següents, d'acord amb el recull que fa la *Guia per a empreses* (Inteco, 2009) del contingut del RDLODP:

"1) Recopilar i descriure les mesures, normes, procediments, regles i estàndards de seguretat adoptats per l'empresa.

2) Determinar l'àmbit d'aplicació del document de seguretat.

3) Establir i comprovar l'aplicació de les normes i procediments del document de seguretat, entre altres, els procediments de notificació, tractament i registre d'incidències, de realització de còpies de seguretat i recuperació de dades, d'identificació i autenticació d'usuaris, d'assignació, distribució i emmagatzematge de contrasenyes, de canvi periòdic de les contrasenyes dels usuaris, de gestió de suports.

4) Elaborar i mantenir actualitzada la llista d'usuaris que tinguin accés autoritzat al sistema informàtic de l'empresa, amb especificació del nivell d'accés que té cada usuari.

Així mateix, establir i comprovar l'aplicació d'un sistema que limiti l'accés dels usuaris únicament a aquelles dades i recursos que necessiten per al desenvolupament de les seves funcions i autoritzats pel responsable del fitxer.

5) Concedir, alterar o anular l'accés autoritzats a les dades i recursos, d'acord amb els criteris establerts pel responsable l'Arxiu.

6) Vetllar pel compliment de les normes de seguretat contingudes en el document de seguretat."

Així i, d'acord amb les característiques del fitxer Gestió *de clients i/o proveïdors*, s'ha optat per escollir la Tècnica en Documentació, que coneix de primera mà alguns clients que poden estar interessats en la digitalització de les seves col·leccions o obres, així com el tipus de suports i programari necessari per desenvolupar el tractament, i com a conseqüència s'ha considerat que és qui millor es pot coordinar amb el propi equip, especialment amb l'administrativa, per tal de fer complir les mesures de seguretat. I s'ha assignat com a administrador del fitxer, l'enginyer informàtic, que coneix de primera línia els processos d'autenticació i gestió de permisos i contrasenyes, figura en qui pot delegar la responsable.

En canvi, per al fitxer *Gestió de personal i nòmines*, s'ha triat l'arxivera de l'equip, per tal com és una usuària avançada del programari específic, que coordina la part del fitxer relacionada amb la prevenció de riscos, i dóna suport a l'arxiu de la documentació de tot el fitxer. I s'ha deixat, en un segon pla, l'administrativa-comptable que tracta a fons amb el contingut del fitxer, com a administradora, figura en qui pot delegar la responsable.

A l'Annex 2 del document de seguretat, es constata que els responsables de Seguretat han estat designats per carta de nomenament.

7.3.3. Mesures de seguretat en funció del nivell requerit

Les mesures de seguretat establertes per la legislació sobre les dades de caràcter personal, es fixen en funció del nivell de seguretat –abans descrit, baix, mig o alt- corresponent al fitxer, i en funció del suport del mateix (automatitzat o no automatitzat). S'han agrupat les mesures, en tres àmbits d'actuació atenent als criteris referits a la gestió i conservació de dades i suports, a la infraestructura de comunicació i criteris d'accés, i al control i revisió de les mesures.

Al document de seguretat de FOTOSIC, s'han previst les mesures de seguretat que ha d'adoptar com a responsable dels seus fitxers. D'altra banda, com a encarregada de tractament, en cas que els seus clients siguin persones físiques, haurà de comprometre's al coneixement i compliment de les mesures de seguretat establertes pel responsable del fitxer que tracta, a través del contracte establert amb ell i que el client haurà previst en el seu document de seguretat, quan tracti els fitxers del client, en els locals de FotoSic i, de vegades, amb accés remot, d'acord amb l'article 82 del RDLODP en aquest sentit pel que fa a les seves condicions d'accés, establertes pel responsable. Com s'ha dit, l'aplicatiu de FotoSic, de moment, s'aplica al tractament del fitxer d'un client corporatiu i no preveu, per tant, aquesta obligació respecte del fitxer del client.

7.3.3.1. Criteris d'arxiu, gestió de suports i preservació de dades

Tot i que el RDLODP només contempla l'obligació d'aplicar criteris d'arxivament per als fitxers no automatitzats, com a mesura de nivell bàsic en el seu article 106, el quadre de classificació de FotoSic preveu també aplicar-ne per als fitxers automatitzats, atesa la seva quantitat més nombrosa d'aquest tipus de fitxers, i la necessitat d'establir criteris homogenis i comprensibles, per tal de garantir-ne la seva localització i consulta, així com una correcta preservació de les dades que contenen.

Pel que fa als suports se seguirà el procediment d'etiquetatge que preveu l'article 92 del RDLODP.

La gestió de suports es fa d'acord amb els articles 92 i 97 del RDLODP, que estableixen mesures de seguretat de nivell bàsic i mitjà respectivament. També s'ha previst el que diu l'article 86 per a les dades que es tractin fora dels locals del responsable del fitxer, quant a la necessària autorització i al nivell corresponent de mesures. D'acord amb aquestes mesures, s'annexen al document de seguretat, models i exemples de l'inventari de suports amb opcions de reutilització i destrucció, el registre d'entrades i sortides de suports, i les autoritzacions corresponents.

Per tant, l'empresa disposa de procediments exposats evidenciats al document de seguretat, que garanteixin la correcta identificació de la informació emmagatzemada en els suports que n'ha de permetre l'accés autoritzat, la sortida de suports dels locals de tractament amb l'autorització del responsable de Seguretat, o el seguiment de les instruccions indicades a l'apartat 2 per tal d'evitar la recuperació de dades en els suports que hagin de ser eliminats.

Les instruccions respecte de la gestió de suports i de les restriccions en la recuperació de dades personals, estan documentades amb els corresponents permisos d'accés, i autoritzacions per a la gestió de suports i recuperació de dades, i són aplicables també al supòsit (com preveu el PT 6 de Velasco Dobaño) per evitar la recuperació de dades personals d'aquells suports que hagin de ser traslladats per dur a terme operacions de manteniment.

L'adequació pràctica del procediment descrit en el document de seguretat, s'haurà de verificar mitjançant l'anàlisi de l'inventari de suports per a quantificar el nombre de jocs de còpies de seguretat existents - PT-7 (Velasco Dobaño, 2005).

Pel que fa a les còpies de seguretat i recuperació de dades, s'han seguit els requeriments previstos per als fitxers automatitzats de nivell bàsic a l'article 94 del RLODP.

7.3.3.2. Criteris d'accés i sistemes de comunicació

Pel que fa als criteris d'accés, com es tracta de mesures per a fitxers, de tractament majoritàriament automatitzat –encara que el de personal sigui mixt-,

i de nivell mitjà, s'ha aplicat la mesura de l'article 98 RDLODP, per limitar la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació.

I d'acord amb l'article 93, per al nivell bàsic, també de tractament automatitzat, el document de seguretat contempla l'evidencia un procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat, així com l'estabilitat inferior a un any per a modificar-les.

Les mesures de control d'accés en funció dels perfils s'han definit i justificat amb detall a l'Annex 1 de l'esmentat document, i inclouen només al personal de FotoSic, que disposa de claus d'identificació individualitzades. Pel que fa a la tramesa de comandes i factures del fitxer *Gestió de clients i/o proveïdors* es farà per correu electrònic. Igualment s'ha identificat el personal autoritzat per concedir, alterar o anul·lar els accessos.

I d'acord amb els papers de treball de Velasco Dobaño (2005) s'ha de comparar la correspondència del llistat actualitzat de recursos, nivells i privilegis d'accés a cada fitxer, amb les funcions dels usuaris abans verificades a través del PT-2 (vegeu Annex 6). Les funcions i obligacions del personal estan previstes als annexos I i X del Document de Seguretat (annex 5), i el llistat de nivells i privilegis d'accés també a l'annex I del Document.

El nivell d'accés als equips del Fitxer d'acord amb les funcions dels usuaris, s'ha classificat segons la següent tipologia d'usuaris:
- *Usuari bàsic:* que utilitza exclusivament el PC assignat, i no està autoritzat per instal·lar-hi programes.
- *Usuari mitjà*: que també utilitza exclusivament l'equip assignat, i a més està autoritzat a instal·lar-hi programes.
- *Usuari avançat:* amb capacitat de realitzar tot tipus de canvis en qualsevol dels equips

Pel que fa al tractament amb qualsevol tipus de suport, i a l'accés a la part del fitxer no automatitzat, també s'han definit a l'apartat 2 del document i les autoritzacions s'han previst als annexos III i IV.

Quant a la infraestructura de l'equipament informàtic prevista a l'inici d'aquest projecte, s'ajusta a les necessitats de la gestió de telecomunicacions definida en el document de seguretat.

En l'annex VII de l'esmentat Document, també es fa constar la clàusula per afegir al contracte amb tercers, com el servei de neteja i el proveïdor de telèfon i d'Internet.

7.3.3.3. Control d'incidències i revisió periòdica

Respecte del registre d'incidències, la plantilla aportada a l'annex IV del document de seguretat, conté els camps mínims exigits per l'art. 90 del RDLODP. Es preveu l'obligatorietat d'omplir tots els camps del registre d'incidències i esbrinar, mitjançant els registres d'activitat d'algunes aplicacions com antivirus, tallafocs i còpies de seguretat, si s'han produït incidències que no incloses. De moment, atesa la recent creació de l'empresa i dels seus fitxers, encara és aviat per fer aquesta comprovació.

Els elements necessaris per al procediment, d'obligat compliment, de la notificació d'incidències, han estat recollits a l'apartat 4 del document de seguretat. La persona a qui s'adreçaran serà la responsable de seguretat de cada fitxer. Per a fitxers de nivell mitjà com els de FOTOSIC, a més hi ha l'obligació d'adjuntar informació sobre el procediment de recuperació de dades (art. 100 del RDLODP). Els camps requerits per aquest procediment s'han afegit al model de registre d'incidències, tret de l'autorització per aplicar la recuperació de dades, habitual o com a mesura correctora, que s'ha adjuntat en l'annex III corresponent a les autoritzacions del responsable del fitxer.

Finalment, també a partir del nivell mitjà de tractament, dels nostres fitxers, cal realitzar una auditoria dels sistemes d'informació i instal·lacions de tractament almenys cada dos anys, d'acord amb els articles 96 i 110 del RDLODP de fitxers automatitzats i manuals respectivament. Al document de seguretat s'ha previst la contractació d'un auditor extern, que en realitzi amb la periodicitat regular establerta, però també d'extraordinàries quan hi hagi modificacions substancials del sistema d'informació que afectin les mesures de seguretat.

Atès que l'empresa FOTOSIC, SL és de nova implantació i la creació dels fitxers és inferior a dos anys, encara no es disposa de cap informe d'auditoria per comprovar l'adopció de les mesures de seguretat. El procés d'anàlisi per a la implementació del compliment de la LOPD reuneix els requisits d'una primera auditoria i l'adopció de les mesures concretes adoptades en són la seva conseqüència.

8. L'encàrrec del fons corporatiu: gestió documental i recomanacions

Com s'ha comentat l'encàrrec de servei de FOTOSIC a la Fundació, no consistirà en el compliment normatiu de protecció de dades personals del seu fitxer, sinó en la gestió i tractament dels documents que n'inclouen les dades, per a la seva consulta i difusió. Per això, FOTOSIC requerirà d'alguna informació prèvia del fitxer del client.

En registrar la comanda de l'encàrrec, FOTOSIC, sl., en primer lloc, demanarà al seu client, en aquest cas, la **Fundació Arquitectes amb l'Habitatge Digne**, les dades que caracteritzen el material a digitalitzar:

Títol
Procedència (fons al qual pertany)
Titularitat del fons
Data /es de la selecció
Volum (unitats)
Mides
Suport
Observacions

Juntament amb aquesta breu descripció, per tal que FOTOSIC pugui determinar el tipus d'actuacions a prendre amb cada peça, la Fundació haurà de dir les fotografies que vol digitalitzar presentades per grups, en funció de l'ordre de prioritats que hagi assignat per a la selecció –semblant a la justificació d'una proposta segons la *Guia de digitalització de* la *Xarxa d'Arxius Comarcals* (2010)-, i atenent a algun dels següents criteris, però emplenant obligatòriament els camps referents als aspectes dels drets:

1. Contingut
2. Demanda
3. Accés
4. Estat físic de la documentació
5. Drets de protecció de dades personals *
6. Drets d'autor *
7. Altres

* Camp a omplir obligatòriament: dir si hi ha aspectes a considerar que poden vulnerar aquests drets, atès que poden limitar l'ús, l'accés i la difusió de la documentació digitalitzada.

Tot seguit, la sol·licitud per part del client, es completarà amb les següents dades:

- Tractament arxivístic establert prèviament en els documents originals: classificació, ordenació, descripció. Es vol mantenir?
- Finalitat de la digitalització i ús que es pretén donar a la documentació digitalitzada –important si es vol difondre a Internet.

En el cas que ens ocupa, la Fundació disposa d'un fons d'unes 60.000 fotografies i ens aporta una col·lecció de prop de 5.000 fotografies agrupades en àlbums, però també alguns pòsters, i retrats emmarcats.

En aquest apartat, es pretén donar una visió general de les actuacions realitzades per FOTOSIC, a partir de la demanda concreta i d'alguns aspectes rellevants dels documents fotogràfics que la Fundació ens fa arribar. Per això, en primer lloc, s'aporta un llistat dels nivells de seguretat requerits per la normativa en matèria de protecció de dades personals i que la Fundació aplica a les seves fotografies. En segon lloc, es complementen aquests requeriments normatius, amb altres entorn de la recollida i la publicació dels documents que contenen les dades. Aleshores, es fa una breu revisió de les actuacions adoptades per FOTOSIC en el procés de digitalització, des del tractament previ fins als criteris d'arxiu i tipus d'emmagatzematge, i finalment, la PIME aporta també algunes recomanacions, per a l'entorn web on es publiquin.

8.1. Nivells de seguretat exigibles en l'encàrrec del fons fotogràfic

Per tal que ens ajustem als paràmetres de digitalització adequats, i els aportem criteris per a la gestió del fons, en la tramesa de material, la Fundació ens fa arribar un quadre orientatiu dels nivells de seguretat que ha aplicat al seu fons. Les mesures que la pròpia Fundació haurà de contemplar, ens donaran una visió de futur a fer la mateixa tasca per a clients finals.

En el cas que ens ocupa, la Fundació ens aporta un fons agrupat en àlbums, però també alguns pòsters, i retrats emmarcats. La Fundació ha fet una selecció de les fotografies que desitja digitalitzar i difondre, i ha demanat a FotoSic que estableixi els criteris d'arxiu que consideri més oportuns per matèria.

Anem a veure quins nivells de seguretat a aplicat la Fundació al seu fons fotogràfic amb dades personals, amb alguns exemples, il·lustratius.

Aplicació de nivells de seguretat exigibles, segons finalitat i ús de les dades:

<table>
<tr><td colspan="2">A. Nivell bàsic
El tipus de mesures que corresponen en aquest nivell, s'hauran d'aplicar a tots els fitxers i tractaments. (art. 81.1 RDLODP)</td></tr>
<tr><td>Retrats que arribin en suport físic de:
- Un noi amb crosses que passava prop de l'edifici;
- Assistents amb el logo i distintius d'una organització o d'un partit polític en unes jornades;
- Un dels assistents a una jornada amb una gorra del Barça;</td><td>Excepció de les de nivell alt art. 81.3, segons art. 81.5:
"En el cas de fitxers o tractaments de dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual només s'han d'implantar les mesures de seguretat de nivell bàsic quan:
a) Les dades s'utilitzin amb l'única finalitat de realitzar una transferència dinerària a les entitats de què els afectats siguin associats o membres.
b) Es tracti de fitxers o tractaments no automatitzats on de forma incidental o accessòria s'incloguin les dades sense tenir relació amb la seva finalitat." – perquè no és la finalitat del fitxer tractar aquests fets.
Nota: i quan es tracti de fitxers automatitzats, sempre i quan les persones no siguin identificables, com es deriva de la LOPD.</td></tr>
<tr><td colspan="2">B. 1. Nivell mitjà</td></tr>
<tr><td>a) La base de dades de clients de FotoSic.
b) Retrats de:
Persones dinant o brindant dins o fora l'edifici; salutacions formals i informals; preparant un esdeveniment; un professional mostrant un obsequi; obrers treballant; donant conferències; en una inauguració …
L'entrega d'habitatges a diferents persones.</td><td>"f) Els que continguin un conjunt de dades de caràcter personal que ofereixin una definició de les característiques o de la personalitat dels ciutadans i que permetin avaluar determinats aspectes de la seva personalitat o comportament" (art. 81.2 RDLODP)</td></tr>
<tr><td colspan="2">C. Nivell alt (art. 81.3 RDLODP)</td></tr>
<tr><td>- reportatge gràfic d'una manifestació sindical d'arquitectes;
- un arquitecte mostrant a la càmera una mà enguixada;
- una membre de l'equip embarassada, a casa seva.</td><td>"a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual".
En els casos dels professionals amb la mà enguixada i en estat, s'entén no es pot aplicar l'art. 81.6 RDLODP, si no es tracta d'una simple declaració de la seva condició per al compliment de deures públics.
D'altra banda, s'entén que són casos en què les persones s'hi han posat voluntàriament, en cas contrari, o que siguin d'informació accessòria per a la finalitat de la imatge, i de suports no digitalitzats, s'aplicarà l'art. 81.5 b esmentat.</td></tr>
</table>

8.2. Què es pot fotografiar i què és publicable?

Atès que el servei de digitalització inclou, sempre a petició del client, la difusió pública de fotografies a Internet, en webs corporatius, blocs i/o xarxes socials, la Fundació haurà d'haver previst prèviament quines imatges es poden capturar i considerar d'aquestes quines i com són publicables d'acord amb allò que en diu la normativa, especialment, la *Llei orgànica 1/1982 de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge*.

D'acord amb l'article 8 d'aquesta llei, no es consideren intromissions il·legítimes, actuacions com: la captació, reproducció o publicació per qualsevol mitjà quan es tracti de persones que tinguin un càrrec públic o una professió de notorietat o projecció pública i la imatge es capti durant un acte públic o en llocs oberts al públic; ni tampoc sobre un succés o esdeveniment públic quan una persona determinada apareix de manera accessòria. Tanmateix es requereix la protecció de l'anonimat en els casos de persones que executen una professió de risc (com les forces o cossos de seguretat de l'Estat), o d'edificis judicials i sales de vista, entre altres.

I en canvi, sí tenen la consideració d'intromissions il·legítimes en l'àmbit de protecció delimitat per l'article 2 de la *Llei orgànica 1/1982*: l'art. 7.5, quan la captació, reproducció o publicació per fotografia de la imatge d'una persona sigui en llocs o moments de la seva vida privada o fora d'aquests, llevat dels esmentats de l'article 8.

Amb tot, caldrà disposar de consentiment per a l'ús de les col·leccions fotogràfiques en què hi apareix la vida professional, privada i familiar, d'acord amb l'article 2 que defineix que cada persona pot mantenir reserves diferents per a ell o per a la seva família. Al mateix temps, no es considerarà intromissió si la persona fotografiada dóna el seu consentiment per accedir a l'àmbit que determini.

Així, sempre que hi hagi habilitació legal, per exemple, mitjançant un consentiment, previ lliure, específic i informat com el que preveu la LODP, serà possible fotografiar al carrer o en espais oberts al públic, o quan es tracta de contextos de rellevància informativa pública.

D'altra banda, caldrà respectar els menors que s'acullen a la *Llei Orgànica 1 / 1996, de 15 de gener, de protecció jurídica del menor i de les disposicions civils vigents*. Segons l'article 4t, el termini de protecció del dret a la pròpia imatge i a la intimitat,

així com el període en què els hereus podran exercir el dret, és de vuitanta anys des de la mort de la persona.

Una altra cosa, és l'ús que se'n fa, si es vol publicar les imatges, per exemple, a Internet. Per tal de fer-les no identificables, i que d'aquesta manera no siguin dades de caràcter personal acollides per la LOPD, la solució exigeix pixel·lar-les i fer anònimes les persones que hi apareixen (vegeu la notícia en altres països sobre l'*streetview* de Google[1]) .

En el supòsit pràctic d'aquest treball, la Fundació com a responsable determinarà si les imatges són publicables –i si no s'incorre en infraccions a la normativa nacional, com en el cas de Lindqvist, en què l'esmentada normativa ha d'adaptar la Directiva europea 95/46/CE en la seva aplicació.

I FOTOSIC, per la seva banda, integrarà en el seus serveis l'anonimització de les dades o el **pixel·lat** de les cares per a la selecció de fotografies que s'hagin de publicar a Internet, d'acord amb el que la Fundació ha previst en la normativa:

- Quan es tracti de fitxers en format digital on de forma incidental o accessòria s'incloguin les dades sense tenir relació amb la seva finalitat.
- Sempre que no es considerin intromissions il·legítimes, a la vida privada o fora d'aquesta, d'acord amb l'art. 7.5 de la *Llei orgànica 1/1982.* Per exemple, en alguna entrega de pis, al seu inquilí o propietari, amb el seu consentiment.
- En tots aquells altres casos, on les persones no s'hi han prestat voluntàriament i/o requereixin aplicar nivells de seguretat de mitjà o alt per tal de fer-les no identificables.

A més de tot això, en el cas no previst que un document formés part del patrimoni documental, caldria tenir en compte, a més, el que diu de l'accés i consulta l'art. 57 de la LPHE i de la Llei 10/2001, de 13 de juliol, d'arxius i documents.

[1] "Google deberá pixelar las caras y matrículas en Street View". *Vida en la Red.* 05.04.2011. A Terra: http://www.terra.es/tecnologia/lared/articulo/suiza-google-street-view-27762.htm

8.3. Tipus d'actuacions: gestió documental i preservació

La gestió documental juntament amb el procés de tractament de la imatge, contribueixen en gran mesura a la protecció de dades, en la mesura que ens ajuden a identificar, quan escau, quins canvis s'han efectuat, i comporten una prova de control per certificar l'autenticitat dels documents.

En finalitzar el seu servei, FOTOSIC adjuntarà amb la documentació original i digitalitzada, un informe sobre l'actuació, que inclourà a més dels apartats del procés explicatiu que s'exposen a continuació, elements com: la identificació sumària de la documentació digitalitzada, els terminis de l'encàrrec, el número de volums i/o pàgines, i els paràmetres acordats. A més hi podrà incloure un qüestionari de satisfacció, amb la valoració sobre el procediment de treball, i el resultat de la digitalització.

Veiem la descripció dels elements del procés.

8.3.a) Tractament abans i després del procés de digitalització

Prèviament a la digitalització caldrà examinar la integritat de l'estat dels documents originals, i quan escaigui, aplicar els següents tractaments físics per augmentar la qualitat de la captura, però per altra també, evitar malmetre l'escàner:

- Extracció d'elements aliens al suport (clips, grapes...)
- Neteja superficial del document
- Protecció del document
- Restauració

Recordem que la integritat contribuirà a identificar correctament els documents, cosa que serà el que ens permetrà determinar-ne l'autenticitat.

Després del procés realitzat, i d'acord amb la *Guia* per als Arxius Comarcals (2010), es poden aplicar processos de millora en aquelles imatges en què es consideri recomanable d'aplicar, sempre que l'augment de la qualitat de l'escaneig de la imatge no suposi una pèrdua considerable de la fidelitat respecte de l'original. Alguns d'aquests tractaments poden ser: neteja i eliminació del soroll; eliminació del moaré; lluminositat i contrast; correcció de la orientació; eliminació de marges; eliminació d'obliqüitat, i negativar o positivar.

En aquesta fase posterior a la digitalització, es procedirà a la pixel·lació de les cares de les fotos seleccionades, mitjançant aplicacions com el Photoshop o el Macromedia Fireworks.

A títol orientatiu, FOTOSIC aplicarà les solucions per garantir la fiabilitat de les imatges escanejades aportades per la norma UNE-ISO/TR 15801:2008 IN “Imagen electrónica. Información almacenada electrónicamente. Recomendaciones sobre veracidad y fiabilidad”.

8.3.b) Emmagatzematge i formats per a la preservació i la consulta

L’estratègia de preservació ha de ser proactiva des de l’estadi més inicial de la vida del material digital. Com assenyala la *Guia* (2010) esmentada, les amenaces contra la pervivència del material digital giren al voltant de tres conceptes: la inestabilitat dels dispositius d’emmagatzematge, l’obsolescència de les tecnologies d’accés i la problemàtica de la integritat i autenticitat del material digital.

Pel que fa a la primera amenaça, els suports magnètics i òptics, en els quals s’emmagatzemen els objectes digitals, es deterioren ràpidament i poden fallar en qualsevol moment per agents externs i ambientals com la calor, la humitat, els contaminants, l’ús intensiu o la manca de cura en la seva manipulació. A més, la seva vida útil és sorprenentment curta. I malgrat això, encara excedeix al temps pel que pot ser llegit i interpretat pel programari o maquinari adequat.

Per tant, l’obsolescència dels programaris d’interpretació i les màquines que fan possible interpretar el material digital compost d’una cadena de bits, encara és un factor més limitant que la durada dels suports esmentats.

A més, l’organització ha de preveure aquests requeriments en el disseny de protocols de conservació a llarg termini amb estratègies com la migració de les dades que sens dubte altera la cadena de bits, i que han de permetre preservar la integritat i autenticitat del material digital. FOTOSIC controla aquest aspecte amb les metadades de preservació, que documenten els processos esdevinguts al llarg del temps (còpies, migracions de format, o qualsevol alteració produïda) d’emmagatzematge al servidor.

En relació amb el primer factor dels suports, s'ha previst com a opcions més segures avui dia, els discs durs externs i en cas que hi hagi un nombre considerable de documents per consultar, el servidor de la Intranet d'accés per al client. D'aquesta manera, es minimitzen també els riscos de pèrdua que podria suposar el trasllat de documents entre els centres.

Abans d'iniciar el procés de captura digital, s'han definit els paràmetres de formats que s'utilitzaran, d'acord amb les finalitats de consulta i/o difusió, a les quals es destinaran els fitxers, i segons tot agafant com a referent l'esmentada *Guia* (2010):

Format: JPEG (consulta) / PDF (difusió)
Resolució: 150 ppp
Profunditat de bits: Gris 8 bits, color 24 bits
Compressió: baixa

8.3.c) Criteris d'arxiu dels fitxers automatitzats

Els criteris d'arxiu ens ajuden a preservar i a localitzar la documentació de forma adient.

La Fundació ha fet una selecció de les fotografies que desitja digitalitzar i difondre, i ha demanat a FotoSic que estableixi els criteris d'arxiu i l'estructura de fitxers digitals que consideri més oportuns, atès que la LOPD només estableix l'obligació per als criteris d'arxiu, i ho fa sobre els fitxers no automatitzats.

Àlbums:

- *Inauguració de l'edifici de la Fundació* (Gener 1985)
- *Obra pública del barri de Can Mates* (1991)
- *Promoció habitatge protegit a Can Caldetes* (1996)
- *1es Jornades sobre el foment de l'habitatge* (1997)
- *Entrega habitatge social a Can Feliu* (Febrer 1998)
- *Reformes habitatge social* (2003-2005)
- *Entrega premis arquitectes fundacionals* (2005)

Pòsters:

- *Retrat de l'equip de la Fundació davant l'edifici* (1985)
- *Inauguració dels primers habitatges de la Fundació* (1987)

Retrat emmarcat:

- *Retrat del fundador* (1986)

FOTOSIC estableix els criteris a partir d'unitats documentals d'àmbit temàtic, que es corresponen majoritàriament amb els àlbums originals. Únicament en el cas de retrats, pòsters o peces que la Fundació li ha presentat soltes, les hi assigna un àmbit temàtic comú, com la resta d'unitats documentals –últim exemple, sobre els "Orígens de la Fundació".

- **Codi tipus d'unitat -** 1 dígit -valor A si la unitat documental no textual, valor B si la unitat és textual, valor C si es tracta d'una unitat és d'instal·lació.
- **Codi de la unitat** - 4 dígits -es correspon amb el codi que atorga l'aplicació a la descripció de la unitat documental que correspon a l'àlbum.
- **Número d'imatges** - 6 dígits

Així, el model d'exemple és:
FUNDAHD A 0000,005000.jpg

Veiem-ne alguns:

Obra pública del barri de Can Mates
(FUNDAHD A 0158,000124.jpg)
1991

Promoció habitatge protegit a Can Caldetes
(FUNDAHD A 0210,000645.jpg)
1996

1es Jornades sobre el foment de l'habitatge
(FUNDAHD A 0401,000701.jpg)
1997

Entrega premis arquitectes fundacionals
(FUNDAHD A 0320,001752.jpg)
2005

Orígens i evolució de la Fundació
(FUNDAHD A 0051,002047.jpg)
1985-2010

L'arbre de carpetes per facilitar la consulta serà com segueix:

Nom de la sèrie / fons
Nom de la unitat documental simple
Pàgines / imatges: nom fitxer. extensió
nom fitxer. Extensió

Per al registre es fan servir els elements descriptius de nivell bàsic del Dublin Core aplicables a qualsevol recurs electrònic, com diu la UNE-ISO 15836:2007 “Informació i Documentació: Conjunt d’elements de metadades Dublin Core”.

8.4. Recomanacions per a la difusió dels documents a Internet

Juntament amb el tractament per a la difusió de les seves fotografies a Internet, com a servei de valor afegit, FOTOSIC proposa a la Fundació, a títol orientatiu, no prescriptiu, algunes pautes de la *Recomanació 1/2008* (ACPD, 2008) sobre la difusió d’informació que contingui dades de caràcter personal a través d’Internet, concretament respecte de les seus electròniques o pàgines web a través d’Internet.

Així, per exemple, es recomana comprovar que els enllaços a la seu electrònica remetin a webs que reuneixin dels requisits de la legislació en matèria de protecció de dades; o contemplar el programari necessari per fer front als atacs malintencionats a través de les comunicacions, que puguin aprofitar les vulnerabilitats de les plataformes col·laboratives.

En aquesta línia i per tal d’evitar riscos en falles de seguretat, a més de les mesures que hagi d’adoptar la Fundació d’acord amb els requeriments normatius, respecte dels fitxers automatitzats a Internet, és convenient establir determinades regles d'ús per al personal (Martínez, 2009b) en relació amb:

- L'ús d’Internet per a tasques no relacionades directament amb les funcions assignades.
- La introducció de continguts a la xarxa corporativa i / o ordinador personal.
- L'enviament de correus massius emprant la direcció de correu electrònic corporativa.
- La instal·lació de programari no autoritzat.

Pel que fa als blocs, tot seguint amb la *Recomanació 1/2008* (ACPD, 2008), cal contemplar, que des del moment que creem un domini propi per allotjar una pàgina personal en què altres usuaris poden deixar els seus comentaris, per exemple sobre les fotografies, ens responsabilitzem dels comentaris establerts per aquests altres usuaris, encara que el responsable últim és la persona que els realitza. Davant del risc de comentaris que atemptin contra l’honor, la pròpia imatge i la intimitat personal, la llei preveu que es pugui exigir a l’autor i de forma ascendent, al

propietari de la pàgina, que remeïn el dany comès a l'afectat amb una rectificació o rèplica. En cas, però de comentaris difamatoris o d'infringir-se algun dret a la pàgina, caldrà recórrer als jutjats i tribunals, atès que la CE en el seu article 20.5 prohibeix el segrest de publicacions, enregistraments i altres mitjans d'informació si no és realitzat en virtut de resolució judicial.

9. Reflexió final: la cultura organitzativa en protecció de dades

En el supòsit pràctic d'aquest treball, s'observa com s'apliquen i articulen un conjunt de normatives en diferents àmbits i escales, per respondre a l'obligatorietat i alhora necessitat de regulació en el tractament de la informació personal en una organització empresarial de serveis vinculats amb els avenços tecnològics de la Societat de la Informació i el Coneixement. Així, a més de la regulació que existeix pròpiament en matèria de protecció de dades, a l'hora d'implementar els serveis de l'empresa, s'ha vist la necessitat de recórrer en determinades circumstàncies a d'altres requeriments normatius, en matèria de drets dels interessats, com Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i del comerç electrònic.

S'ha pogut observar també com l'adopció de les mesures que requereix la normativa, estan estretament relacionades amb l'àmbit tècnic, però també organitzatiu. La normativa en protecció de dades contempla l'adopció de les mesures en funció dels dispositius tecnològics, però també preveu l'assignació de funcions i obligacions del personal i eines per a la comunicació. I crec que si bé no integra el concepte de treball en xarxa, bastant lluny encara de moltes organitzacions, en canvi, permet facilitar l'assignació de responsabilitats, la coordinació i el compromís de l'equip.

Si bé en la Societat de la Informació els aspectes tecnològics i els organitzatius es complementen, i l'àmbit jurídic abordat sembla partir d'aquesta realitat. I qualsevol política de seguretat d'una empresa, ha de preveure tots aquests àmbits per tal que la implementació dels requeriments normatius i les mesures en matèria de protecció de dades, suposin una oportunitat de millora del negoci. A més, cal considerar que l'ordenació i sistematització de la informació que es requereix en el procés, juntament amb els processos de revisió continus, ajuden a detectar problemes o mancances en matèria de seguretat de les dades.

Per tot això, l'adaptació d'una organització laboral per al compliment de la LOPD necessita anar acompanyada d'una sensibilització per part de tot l'equip, que ha de

permetre una cultura de qualitat en el tractament de les dades, dels documents i dels suports que les contenen i de la gestió del negoci, per tal de millorar els processos de gestió de la informació. No es tracta, doncs, simplement de disposar de l'equipament i de la infraestructura material i humana, per dur a terme l'aplicació simple de la normativa, sinó de tenir la cultura organitzativa prèvia per tal de dotar l'organització i detectar els nivells de seguretat requerits per posar en funcionament les mesures en el seu context.

Tanmateix, haurem de preveure alguns possibles problemes que sorgeixen entorn de la cultura organitzativa com assenyala el professor Martínez (2009b):

- Sovint es concep la seguretat com una cosa extraordinàriament costosa, en bona part pel desconeixement que hi ha de les mesures, i no es fa l'adequada inversió en l'estat d'actualització dels equips i del programari. Moltes vegades el responsable del fitxer compta amb programes molt bàsics que no reuneixen les especificacions de seguretat que corresponen al nivell del fitxer.
- La percepció per part de l'usuari del sistema d'informació, que la RDLOPD és d'una càrrega "excessiva", sense interioritzar els beneficis de l'aplicació de les mesures de seguretat, com la millora de les condicions de treball i la qualitat de la informació.
- S'oblida que la seguretat afecta totes les formes d'informació i els seus suports, així com a qualsevol mètode usat per a transmetre coneixement, dades i idees. Per tant, l'aplicació del RDLOPD no només pot concebre des d'una perspectiva de costos ja que es tracta de quelcom valuós en si mateix.

Una bona comunicació de les polítiques de seguretat al personal, a través de la formació i de la documentació dels processos, crec que és el pas previ i necessari perquè l'equip de personal d'una empresa accedeixi a conèixer la cultura de compliment normatiu en matèria de protecció de dades. I com diu Martínez (2009b), cal interioritzar estratègicament certs valors, com per exemple, els que aporta la seguretat que permet generar la confiança sobre la capacitat dels sistemes d'informació, a personal i a clients, i en l'eficiència en la gestió d'informació.

El supòsit pràctic d'aquest treball m'ha permès analitzar, d'una banda els requeriments normatius en matèria de protecció de dades que ha de complir una petita empresa de serveis en la societat de la informació i el coneixement, i de l'altra, com a professional

de l'àmbit de la Documentació i des de la perspectiva de mercat que s'obre amb els serveis de digitalització i gestió de documents que s'adrecen habitualment a fons corporatius, comprendre quina és la normativa que s'articula per garantir el dret a informar en aquesta casuística.

10. Bibliografia i webgrafia:

Guies, recomanacions, plans i articles

Agència Catalana de Protecció de Dades (2008): *Recomanació 1/2008 sobre la difusió d'informació que contingui dades de caràcter personal a través d'Internet*. [Data de consulta: 21/03/2011]. Disponible a: http://www.apd.cat/ca/articlesPage.php?cat_id=28&art_id=49

Agencia Española de Protección de Datos (2010): *Guía modelo del Documento de Seguridad.* [Data de consulta: 20/05/2011]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.doc

Agencia Española de Protección de Datos. "2008 0129 La digitalización de la información por una empresa la convierte en encargado del tratamiento". [Data de consulta: 20/05/2011]. Informe jurídic disponible a: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0129_La-digitalizaci-oo-n-de-la-informaci-oo-n-por-una-empresa-la-convierte-en-encargado-del-tratamiento.pdf

Agencia Española de Protección de Datos (2008): *Manual del formulario electrónico de notificación de ficheros de titularidad privada*. Última versió: 20 de maig de 2008. [Data de consulta: 20/05/2011]. Disponible a: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/obtencion_formulario/common/pdfs/ManualdelformularioelectronicoNOTATitularidadPRIVADA.pdf

Berman, P. S. (2007) "Global Legal Pluralism". Southern California Review, Vol. 80, p. 1155; Princeton Law and Public Affairs Working Paper No. 08-001. [Data de consulta: 18/03/2011]. Disponible en línia a: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985340&rec=1&srcabs=1010105

Biblioteca Nacional de Australia (2003): *Directrices para la preservación del patrimonio digital*. [Cap. 16: Protección de datos]. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). [Data de consulta: 18/03/2011]. Disponible a: http://portal.unesco.org/ci/en/ev.php-URL_ID=13271&URL_DO=DO_TOPIC&URL_SECTION=201.html

Bustelo, C. (2008?): Gestión de Documentos y aplicaciones: Introducción. Madrid: AENOR.

CCSDS (2009): *Reference model for an open archival information system (OAIS): Draft recommended standard*. [Data de consulta: 21/03/2011]. Disponible a:

http://public.ccsds.org/sites/cwe/rids/Lists/CCSDS6500P11/Attachments/650x0p11.pdf

Conferencia de Archiveros de Universidades Españolas. *La gestión de documentos electrónicos: recomendaciones y buenas prácticas para las Universidades. Abril 2007.* [Data de consulta: 18/03/2011]. Disponible a: http://cau.crue.org/export/sites/Cau/Quehacemos/gruposdetrabajo/documentoselectronicos/recomendaciones2007.pdf

Doctodata (2008): Pla de digitalització de la cultura a Catalunya: informe diagnòstic, maig 2008, p. 118-121. Disponible a: http://www20.gencat.cat/docs/Biblioteques/Tematic/Documents/Arxiu/Noticies/digitalitzacio_cultura_catalunya/Informe_diagnostic.pdf

European Commission. Secretariat (2009): *Implementing rules for document management and electronic and digitised documents.* Novembre 2009. [Data de consulta: 17/03/2011]. Disponible a: http://ec.europa.eu/transparency/archival_policy/docs/edomec/2009-1643-sec_mda_en.pdf

Esquema nacional de seguridad en el ámbito de la administración electrónica. Regulado por el real decreto 3/2010, de 8 de enero. [Data de consulta: 17/03/2011]. Disponible a: http://www.csae.map.es/csi/pg5e42.htm

Guia de digitalització de la Xarxa d'Arxius Comarcals. De la Subdirecció General d'Arxius i Gestió Documental, Generalitat de Catalunya. 2010. [Data de consulta: 17/05/2011]. Disponible a: http://www20.gencat.cat/docs/CulturaDepartament/DGPC/Arxius_i_Gestio_Documental/06_Plans%20d%27actuacio_documentacio_tecnica/documentacio_tecnica/Guia%20de%20digitalitzacio_v3_definitiva_CC.pdf

Inteco (2009): *Guía para empresas: cómo adaptarse a la normativa sobre protección de datos.* [Data de consulta: 22/03/2011]. Disponible a: http://www.inteco.es/Seguridad/Observatorio/manuales_es/GuiaManual_LOPD_pymes

Inteco (2011): *Resum de la Guia d'introducció al Web 2.0: aspectes de privacitat i seguretat a les plataformes col·laboratives*. Febrer 2011 [Data de consulta: 18/03/2011]. Disponible a: http://www.inteco.es/file/rs2pJgDFDo8T7jcjbxYNVQ

Joint Information Systems Committee (2008): *JISC Programme Synthesis Study: Supporting Digital Preservation & Asset Management in Institutions*. [Data de consulta: 18/03/2011]. Disponible a: http://www.jisc.ac.uk/whatwedo/programmes/preservation/assetmanagement

Navas Fernández, M. (2010): "Centre de Documentació de l'Agència Catalana de Protecció de Dades". A: Jornades Catalanes d'Informació i Documentació (12es: 2010: Barcelona). Col·legi Oficial de Bibliotecaris-Documentalistes de Catalunya. [Data de consulta: 16/03/2011]. Disponible a: http://eprints.rclis.org/bitstream/10760/14851/1/NAVAS_centre_documentacio_APD.pdf

Norma ISO 30300. http://www.iso30300.es/ Iniciativa d' Ebla Gestió Documental

Pla estratègic del servei d'arxiu i registre de la Universitat d'Alacant. Disponible a: http://sar.ua.es/va/documentos/qualitat/planes-estrategics/pla-estretegic-del-servei-d-arxiu-i-registre-2007-2011.pdf

Peguera Poch, Miquel (2006): "Servicios de la Sociedad de la Información: Su caracterización Legal en Europa". Revista de Derecho Informático: Alfa-Redi. Núm. 100. [Data de consulta: 11/04/2011]. Disponible a: http://www.alfa-redi.org/rdiarticulo.shtml?x=7842 .

Rodríguez Gómez, A.; Cristina Biescas Socias (2010): Compendi sobre l'accés a la informació i la protecció de dades. Barcelona: Generalitat de Catalunya. Comissió Nacional d'Accés, Avaluació i Tria Documental. [Data de consulta: 23/03/2011]. Disponible a: http://www20.gencat.cat/docs/CulturaDepartament/DGPC/Arxius_i_Gestio_Documental/01_Sistema_Arxius_Catalunya/Organs_administracio/CNAATD/Banner/2010-11-03_Compendi%20acces%20proteccio%20dades11.pdf

Sentencia del Tribunal de Justicia, de 6 de noviembre de 2003. Suecia, caso Linqdvist. Decisión prejudicial de interpretación de la Directiva 95/46. http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=es&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET

Velasco Dobaño, J.; E. Sanmartí Giménez (2006): *Metodologia de l'auditoria de seguretat.* Barcelona: Agència Catalana de Protecció de Dades. [Data de consulta: 19/03/2011]. Disponible a: http://www.apd.cat/ca/articlesPage.php?cat_id=28&art_id=17

Velasco Dobaño, J; Velasco Masip, L. (2005): Auditoría de la protección de datos. Barcelona: Bosch.

Vives-Gràcia, J. (2007): "Confidencialidad y derechos de autor en un proyecto de intranet". *El profesional de la información,* v.16, n. 3, mayo-junio 2007. [Data de consulta: 21/03/2011]. Disponible a: http://upcommons.upc.edu/e-prints/bitstream/2117/1620/1/vives_confidencialidadderechos.pdf

Legislació:

Carta de Drets Fonamentals de la Unió Europea (2007/C 303/01). A: *Diario Oficial de la Unión Europea.* 14.12.2007. Parlament Europeu. [Data de consulta: 10/06/2011]. Disponible a: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:ES:PDF

Constitució espanyola 1978. [Data de consulta: 23/03/2011]. Disponible a: http://www.parlament.cat/activitat/constitucio.pdf

Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la proteccion de las personas con respecto al tratamiento automatizado de datos de caracter personal. [Data de consulta: 10/06/2011]. Disponible a: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/convenios/common/pdfs/convenio_108_consejo_europa.pdf

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. A: *Diario Oficial n° L 281 de 23/11/1995* p. 0031 – 0050. [Data de consulta: 23/03/2011]. Disponible a: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML

Estatut d'autonomia de Catalunya (2006) [Data de consulta: 23/03/2011]. Disponible a: http://www.parlament-cat.net/porteso/estatut/eac_ca_20061116.pdf

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Versión consolidada no oficial, a 31 de diciembre de 2007. [Data de consulta: 12/04/2010]. Disponible a: http://www.mityc.es/dgdsi/lssi/normativa/DocNormativa/Ley34_02Consolidado_Enero2008.pdf

Llei 9/1993 del patrimoni cultural català (LPCC). [Data de consulta: 12/04/2010]. Disponible a: http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Documents/Arxiu/normativa_index.htm%20-%20LLEI_9_1993.doc

Llei 1/1982 de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge. http://www.afmontcada.com/documents/LO_1-82_intimidad_imagen_honor.pdf

Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. (BOE 298, de 14-12-1999.) [Data de consulta: 14/03/2011]. Disponible a: http://www.boe.es/boe_catalan/dias/1999/12/30/pdfs/A01399-01411.pdf

Llei 16/1985 del Patrimoni Històric Espanyol (LPHE). (BOE de 29.06.1985) [Data de consulta: 14/03/2011]. Disponible a: http://www.mcu.es/bibliotecas/docs/Articulo66PHE.pdf

Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. [Data de consulta: 12/04/2010]. Disponible a: http://www.gencat.cat/eadop/imatges/5731/10273092.pdf

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. (BOE-A-2010-1331). [Data de consulta: 21/03/2011]. Disponible a: http://www.csae.map.es/csi/pdf/RD_3_2010_texto_consolidado.pdf

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. (BOE-A-2010-1331). [Data de consulta: 21/03/2011]. Disponible a: http://www.csae.map.es/csi/pg5e41.htm

Real Decreto 1289/1999, de 23 de julio, por el que se crea la Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías en España. [Data de consulta: 21/05/2011]. Disponible a: http://www.boe.es/boe/dias/1999/07/27/pdfs/A27810-27811.pdf

Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal. [Data de consulta: 21/03/2011]. Disponible a: http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (BOE-A-2008-979). [Data de consulta: 10/03/2011]. Disponible a: http://www.boe.es/boe_catalan/dias/2008/01/19/pdfs/BOE-A-2008-979-C.pdf

Reial decret 1671/2009, de 6 de novembre, pel qual es desplega parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciudadans als serveis públics. *BOE: Suplement en llengua catalana al núm. 278*. [Data de consulta: 21/03/2011]. Disponible a: http://www.boe.es/boe_catalan/dias/2009/11/18/pdfs/BOE-A-2009-18358-C.pdf

Mòduls previs

Martínez Martínez, R. [2005]: *Protección de datos de carácter personal en la Sociedad de la Información*. Barcelona: FUOC. 4 mòduls.

Martínez Martínez, R. (2009a): "El dret fonamental a la protecció de dades". Cerrillo, A. (2009): *Les transformacions del dret a la societat de la informació*. Barcelona: FUOC.

Martínez Martínez, R. (2009b): [Módulo 4. Medidas de seguridad]. *Aplicación de las medidas de seguridad a los ficheros y tratamientos de datos personales: especial atención al Reglamento de Medidas de Seguridad*.

Webgrafia en la matèria:

AENOR. http://www.aenor.es/aenor/inicio/home/home.asp

Agencia Española de Protección de Datos. http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Autoritat Catalana de Protecció de Dades. http://www.apd.cat/ca/index.php

Consejo Superior de Administración electrónica. http://www.csae.map.es/

[Diputació de Barcelona]: Seu electrònica. https://seuelectronica.diba.cat/

ICTnet: Comunidad de Gestión en Seguridad de la Información. http://ictnet.es/administracion/gestion-de-la-seguridad-de-la-informacion

INTECO: Instituto Nacional de Tecnologías de Comunicación. http://www.inteco.es/

JISC: Digital Preservation and Asset Management. http://www.jisc.ac.uk/whatwedo/programmes/preservation/assetmanagement

UNESCO: E-heritage. http://portal.unesco.org/ci/en/ev.php-URL_ID=1539&URL_DO=DO_TOPIC&URL_SECTION=201.html

Altres fonts per documentar l'escenari:

Artyplan solucions en comunicació: tot en producció gràfica. http://www.artyplan.com/cat/home/home.php

HP: España. http://www8.hp.com/es/es/home.html

Iris: OCR Software and Document Management solutions. http://www.irislink.com/c2-646-189/I-R-I-S----OCR-software-and-Document-Management-solutions.aspx

Kernel Doc: Escaneo digitalización documentos. http://www.kerneldoc.net/

Laboratori digital Barcelona. http://www.egm.es/cat/servicios

Servei tècnic Apple. http://www.microgestio.es/cat/super-home.php

Sitio Oficial Dell: España. http://www.dell.es/