INFORME D'AUDITORIA DE PROTECCIÓ DE DADES PERSONALS

COL·LEGI OFICIAL D'INFERMERIA DE BARCELONA

JUNY 2010

PROTOCOL NÚMERO 6198

Índex

1. Introducció

El present informe s'elabora dins del marc legal establert per la normativa de protecció de dades, que exigeix la revisió i adequació dels fitxers automatitzats i no automatitzats que contenen dades de nivell mitjà i alt, conforme al que estableixen els articles 95 a 114 del RD 1720/2007, que aprova el Reglament que desenvolupa la LOPD 15/1999.

Dins la tasca portada a terme per la Unió Catalana d'Hospitals de millora contínua en matèria de protecció de dades, amb adaptació al món sanitari, enguany s'inicia una nova etapa en què les entitats adherides al Codi tipus es sotmeten a una auditoria en aquesta matèria.

Aquesta auditoria s'ha portat a terme per *Faura-Casas, Auditors i Consultors*, qui ha col·laborat des dels inicis en l'assessorament i implantació del Codi tipus.

2. Objectius i contingut de l'auditoria

De conformitat amb el que estableix la normativa sobre protecció de dades, totes les entitats que disposin de fitxers automatitzats i no automatitzats que continguin dades de nivell mitjà i/o alt, hauran de sotmetre, de forma biennal, els seus sistemes d'informació i instal·lacions de tractament de dades a una auditoria.

Com a resultat de l'auditoria s'ha elaborat el present informe que dictamina quines deficiències té el sistema i quines són les propostes de millora.

En aquest sentit es pronuncia l'article 96 del RD 1720/2007 en referència als fitxers automatitzats:

1. A partir del nivell mitjà els sistemes d'informació i instal·lacions de tractament i arxivament de dades es sotmetran, almenys cada dos anys, a una auditoria interna o externa que verifiqui el compliment del present títol.

Amb caràcter extraordinari s'haurà de realitzar l'esmentada auditoria sempre que es realitzin modificacions substancials en els sistema d'informació que puguin repercutir en el compliment de les mesures de seguretat implantades per tal de verificar l'adaptació, l'adequació i eficàcia de les mateixes. Aquesta auditoria inicia el còmput de dos anys assenyalat en el paràgraf anterior.

2. L'informe d'auditoria haurà de dictaminar sobre l'adequació de les mesures i controls a la Llei i el seu desenvolupament reglamentari, identificar les seves deficiències i proposar les mesures correctores o complementàries necessàries. Haurà d'incloure, igualment, les dades, fets i observacions en què es basin els dictàmens assolits i les recomanacions proposades.

3. Els informes d'auditoria seran analitzats pel responsable de seguretat competent, que elevarà les conclusions al responsable del fitxer o tractament perquè adopti les mesures correctores adequades i quedaran a disposició de l'Agència Espanyola de Protecció de Dades o, en el seu cas, de les autoritats de control de les comunitats autònomes.

I també l'art. 110 del Reglament 1720/2007 respecte dels no automatitzats: *Els fitxers compresos a la present secció se sotmetran, almenys cada dos anys, a una auditoria interna o externa que verifiqui el compliment del present títol.*

3. Dades de l'entitat auditada

Dades identificatives

Entitat	COL·LEGI OFICIAL D'INFERMERIA DE BARCELONA
NIF	Q0866003G
Domicili	Carrer Pujades, 350 local, Barcelona (08019)

Data de realització de l'auditoria

Dies	3 i 4 de Juny de 2010

Persones entrevistades

Entrevista 1	Sr. Gabriel Bronchales Auditor Intern
Entrevista 2	Sr. Jordi Fernández Responsable del Departament IT de SOFTENG S.L.
Entrevista 3	Sr. David Rangel Tècnic del Departament IT de SOFTENG S.L.
Entrevista 4	Sra. Núria Balaguer Responsable de Formació

Entrevista 5	Sra. Sònia Navarro Secretària Administrativa de Formació
Entrevista 6	Sra. Raquel Beltrán Responsable de la revisió d'expedients col·legials
Entrevista 7	Sr. Jordi Cardila Responsable d'Arxiu
Entrevista 8	Sra. Isabel Quintana Responsable d'Àrea d'Atenció al Col·legiat
Entrevista 9	Sra. Núria Garcia Adjunta a Gerència
Entrevista 10	Sra. Gemma Bruna Responsable de Comunicació
Entrevista 11	Sra. Dolors Agulló Responsable del Programa Retorn
Entrevista 12	Sra. Laura Rausell Administrativa
Entrevista 13	Sr. Manel Tomás Responsable de Cooperació

A més a més, s'han realitzat comprovacions mitjançant mostreig en els taulells d'informació de les diferents vies d'entrada, al servei de sistemes d'informació (sala de servidors), així com a totes les àrees en les que es fan tractaments de dades de caràcter personal.

4. Metodologia

Per portar a terme l'auditoria s'ha realitzat una revisió *in situ* de les instal·lacions de tractament de dades i sistemes d'informació de l'entitat **COL·LEGI OFICIAL D'INFERMERIA DE BARCELONA**.

Tant el treball d'auditoria com l'elaboració d'aquest informe han sigut desenvolupats per un equip de persones constituït per professionals qualificats en el camp de la protecció de dades de Faura-Casas, treballant de forma simultània els aspectes tècnics i organitzatius de la seguretat, així com també els legals.

Per portar a terme l'execució de l'encàrrec d'auditar el Centre, s'han efectuat les següents actuacions:

- ✓ Realització de l'auditoria a través d'entrevistes, qüestionaris, recopilació i supervisió de documents, i anàlisi i revisió de les mesures, controls i procediments de l'entitat.
- ✓ Elaboració del present informe d'auditoria.

El treball d'auditoria s'ha desenvolupat complint els terminis pactats, i s'ha dividit en les fases que s'indiquen a continuació:

- Identificació dels interlocutors
- Recollida de la informació
- Estudi i anàlisi de la informació
- Aclariments
- Lliurament de l'informe provisional
- Correccions i aclariments sobre l'informe provisional
- Lliurament de l'informe definitiu

5. Punts objecte de revisió

En el desenvolupament dels treballs s'han revisat els següents aspectes:

5.1. Aspectes generals

S'ha comprovat que el responsable del fitxer i/o encarregat de tractament hagi implantat les mesures de seguretat exigibles en base als nivells de seguretat bàsic, mitjà i alt.

5.2. Encarregat/s de tractament

S'ha comprovat si existeix un o diversos encarregats de tractament que prestin serveis a compte del responsable del fitxer i si es prenen les mesures de seguretat legalment exigibles.

5.3. Prestació de serveis sense accés a dades personals

S'ha comprovat que s'hagi limitat l'accés a dades personals a persones que no en necessitin per raó de la seva activitat.

5.4. Delegació d'autoritzacions

S'ha comprovat si s'ha delegat a altres persones la presa de decisions en relació a les mesures de seguretat en relació a les dades de caràcter personal i si aquestes han estat degudament autoritzades.

5.5. Accés a dades a través de xarxes de comunicacions

S'ha comprovat si existia un accés a dades a través de xarxa de comunicacions, i en cas afirmatiu s'ha procedit a verificar si s'ha implantat un nivell de seguretat equivalent al dels accessos en mode local.

5.6. Règim de treball fora dels locals d'ubicació

S'ha comprovat si s'ha donat algun cas de tractament de dades fora dels locals d'ubicació dels fitxers i, en cas afirmatiu, si s'ha autoritzat tal tractament prèviament i de forma expressa pel responsable del fitxer.

5.7. Fitxers temporals

S'ha comprovat si existeixen fiters temporals i, en cas afirmatiu, s'ha procedit a inspeccionar i verificar que aquests fitxers compleixen amb les mesures de seguretat adequades, en funció del nivell de les dades que contenen.

També s'ha verificat si un cop deixen de ser necessaris, aquests fitxers s'esborren.

5.8. Contingut mínim del document de seguretat

S'ha comprovat si el Document de Seguretat tenia el contingut mínim que la normativa estableix com a obligatori. Aquest contingut mínim, en el cas dels fitxers de nivell alt, és:

Contingut Document de Seguretat Fitxers de nivell alt
Àmbit d'aplicació del document
Mesures, normes i procediments per a garantir la seguretat: - Relació d'usuaris autoritzats - Contrasenyes que garanteixen la confidencialitat i integritat - Control d'accés a usuaris no autoritzats - Inventari de suports informàtics en llocs d'accés per personal autoritzat Còpies de seguretat setmanalment Mecanismes que garanteixin la seguretat durant el transport de suports Ubicació física de les còpies en llocs diferents als d'ubicació dels equips La transmissió de dades per mitjans telemàtics haurà de ser encriptada
Funcions i obligacions del personal
Estructura dels fitxers i descripció dels sistemes d'informació que s'utilitzen
Procediment de notificació, gestió i resposta de les incidències
Identitat del responsable/s de seguretat
Mesures, normes i procediments per garantir el nivell mínim de seguretat exigit: - Identitat dels usuaris que intenten accedir al sistema d'informació - Limitació i control d'accés físic als locals a on estiguin ubicats els sistemes de informació i d'arxiu.
Controls periòdics per verificar el compliment del document de seguretat (auditoria

interna o externa cada dos anys)

Procediments d'aplicació pels usuaris que ja no seran utilitzats

Registre de les incidències:

- Procediments de recuperació de les dades
- Persona que executa aquest procediment
- Dades restaurades i dades gravades manualment.

Establiment de registres d'entrada i sortida dels suports informàtics.

Prohibició de realitzar proves amb dades reals.

Establiment d'un registre d'accessos:

- Identitat de l'usuari que té accés, data i hora, fitxer accedit i tipus d'accés
- Manteniment del registre com a mínim durant dos anys.

Quan existeixi un tractament de dades per compte de tercers, s'haurà de contenir la identificació dels fitxers o tractaments que es tractin en concepte d'encàrrec amb referència expressa al contracte o document que reguli les condicions d'aquest encàrrec, així com la identificació del responsable i el període de vigència de l'encàrrec.

En aquells supòsits que el tractament s'incorpori o tracti exclusivament en els sistemes de l'encarregat, el responsable ho haurà d'anotar al DS. Quan aquesta circumstància afectés a part o a la totalitat dels fitxers del responsable, es podrà delegar a l'encarregat portar el DS, excepte en el referent als recursos propis. Aquest fet s'indicarà de forma expressa en el contracte d'encarregat de tractament.

5.9. Funcions i obligacions del personal

S'ha comprovat si estan clarament definides les funcions i obligacions de cada una de les persones amb accés a les dades de caràcter personal i als sistemes d'informació.

5.10. Registre d'incidències

S'ha comprovat si existeix un procediment de notificació i gestió d'incidències.

En cas afirmatiu, s'ha procedit a l'estudi d'aquest procediment i a la verificació e si inclou els punts que la normativa considera imprescindibles com és: la inclusió d'un registre d'incidències on queda constància del tipus d'incidència, el moment en què s'ha produït, la persona que realitza la notificació, a qui se li comunica i els efectes que s'han derivat de la mateixa.

També si existeix un procediment de recuperació de dades que inclogui l'autorització prèvia per escrit del responsable del fitxer, la descripció dels procediments realitzats de recuperació de dades, la indicació de la persona que va executar el procediment, la

descripció de les dades restaurades i quan sigui el cas, la descripció de les dades que hagi estat necessari gravar manualment en el procediment de recuperació.

5.11. Control d'accés

L'auditoria també ha verificat si l'accés per part dels usuaris queda limitat als recursos que necessiten pel desenvolupament de les seves funcions i, en cas afirmatiu, si existeixen mecanismes per evitar que un usuari pugui accedir a recursos diferents als autoritzats.

S'ha inspeccionat si la relació d'usuaris detalla a quins recursos tenen accés i si existeix un llistat del personal autoritzat deforma expressa per alterar l'accés autoritzat als recursos.

També s'ha comprovat si només el personal autoritzat en el document de seguretat té accés físic als locals on es troben ubicats els sistemes d'informació on es contenen les dades de caràcter personal.

5.12. Gestió de suports

S'ha comprovat si els suports informàtics permeten identificar el tipus d'informació que contenen i ser inventariats, si s'emmagatzemen en un lloc amb accés restringit al personal que està autoritzat al document de seguretat i si es produeix la sortida de suports fora del local on està ubicat el fitxer.

En cas que existeixin sortides, s'ha verificat si aquestes sortides es troben expressament autoritzades pel Responsable del fitxer i si existeix un registre d'entrada i sortida dels suports que permeti conèixer el tipus de suport, la data i l'hora, l'emissor, el nombre de suports, el tipus d'informació que conté, la forma d'enviament i la persona responsable del lliurament o recepció.

També s'ha verificat si es prenen les mesures necessàries per garantir que sigui impossible recuperar la informació dels suports reutilitzats.

I s'ha comprovat que la distribució de suports es realitza xifrant les dades o de qualsevol altra forma que les faci inintel·ligibles.

5.13. Identificació i autenticació dels usuaris

S'ha comprovat si existeix una relació actualitzada dels usuaris que poden accedir al sistema i dels procediments d'identificació i autenticació d'aquests accessos.

En cas afirmatiu, i sempre que el procediment d'autenticació s'hagi basat en contrasenyes, s'ha verificat si existeix un procediment d'assignació, distribució i emmagatzematge que en garanteixi la integritat i confidencialitat. També s'ha comprovat si aquestes contrasenyes es canvien com a mínim un cop a l'any.

I finalment, també s'ha verificat que les contrasenyes s'emmagatzemin de forma inintel·ligible i que existeixi un sistema que permeti identificar de forma inequívoca i personalitzada a tot aquell usuari que intenti accedir al sistema d'informació i la verificació a què està autoritzat.

5.14. Còpies de recolzament i recuperació

S'ha comprovat si existeix la descripció dels procediments de realització de còpies de recolzament i recuperació de forma que es garanteixi la reconstrucció de les dades en l'estat en què es trobaven en el moment de produir-se la pèrdua o destrucció de les mateixes, si es realitzen còpies de seguretat amb una freqüència mínima setmanal i si es verifica almenys cada 6 mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies i recuperació de dades.

I s'ha verificat que es conserva una còpia de seguretat i dels procediments de recuperació de les dades en un lloc diferent on es troben ubicats els equips que tracten les dades.

5.15. Registre d'accessos

S'ha comprovat si s'ha creat un registre d'accessos, on es guarda la identificació de l'usuari, la data i l'hora en què es va realitzar, el fitxer accedit, el tipus d'accés i si l'accés s'ha autoritzat o denegat. En el cas dels accessos autoritzats s'ha comprovat si es guarda la informació que permet identificar el registre accedit, durant un mínim de dos anys i si hi ha una revisió mensual de la informació de control registrada.

5.16. Transmissió de dades a través de xarxes de telecomunicacions

S'ha verificat si es transmeten dades a través de xarxes de telecomunicacions, i en cas afirmatiu si es transmeten xifrades o de qualsevol altra forma que faci que sigui inintel·ligible i no pugui ser manipulada per tercers.

Un cop inspeccionats tots els punts descrits a través de la revisió de documents, sistemes i entrevistes a usuaris, s'ha procedit a emetre el següent informe.

5.17. Auditoria

S'ha comprovat si els sistemes d'informació que tracten dades de nivell mitjà i alt es sotmeten a una auditoria interna o externa almenys cada 2 anys i si els informes d'auditoria que se'n deriven dictaminen les diferències i les mesures correctores en el tractament de dades personals.

5.18. Criteris d'arxiu

S'ha comprovat si l'arxiu dels suports i documents es realitza d'acord amb els criteris que estableixi la normativa sectorial de referència, i si en tot cas es garanteix la correcta conservació dels documents.

Un cop inspeccionats els punts descrits a través de la revisió de documents, sistemes i entrevistes a usuaris, s'ha procedit a emetre el següent informe.

6. Anàlisis de les diferents àrees de l'auditoria

PREVI:

El COL·LEGI OFICIAL D'INFERMERIA DE BARCELONA és una institució que vetlla per la defensa i representació corporativa de les infermeres i els infermers, i pretén generar valor social i professional al col·lectiu i alhora contribuir a millorar l'atenció sanitària, sociosanitària i social a Catalunya.

És una corporació de dret públic d'estructura democràtica, les principals funcions del qual són la defensa dels interessos professionals dels seus col·legiats i col·legiades i el vetllar perquè l'activitat professional es desenvolupi sota els principis de la bona praxi, adequant-se a l'interès públic general.

El Col·legi està dotat d'uns estatuts que regulen el seu funcionament, d'acord amb la Constitució, l'Estatut d'Autonomia de Catalunya i la Llei de Col·legis Professionals. Segons aquesta normativa, cal que totes les infermeres i els infermers que exerceixen la professió, en qualsevol de les seves modalitats, dins de l'àmbit territorial de la demarcació de Barcelona, hi estiguin adscrits.

Tant les mesures de seguretat emprades com la documentació acreditativa seran objecte d'anàlisi en els apartats successius, no obstant, és important comentar que el fet que l'entitat disposi de la ISO ha suposat que molts documents de protecció de dades hagin canviat de nomenclatura per tal d'adaptar-los a les normes d'aquest estàndard de qualitat.

6.1. Aspectes generals

Article 79 RDLOPD.- *Els responsables dels tractaments o els fitxers i els encarregats del tractament han d'implantar les mesures de seguretat d'acord amb el que disposa aquest títol, amb independència de quin sigui el seu sistema de tractament.*

Article 80 RDLOPD.- *Les mesures de seguretat exigibles als fitxers i tractaments es classifiquen en tres nivells: bàsic, mitjà i alt.*

Article 81 RDLOPD.- *1. Tots els fitxers o tractaments de dades de caràcter personal han d'adoptar les mesures de seguretat qualificades de nivell bàsic.*

2. S'han d'implantar, a més de les mesures de seguretat de nivell bàsic, les mesures de nivell mitjà, en els següents fitxers o tractaments de dades de caràcter personal:

a) Els relatius a la comissió d'infraccions administratives o penals.

b) Aquells el funcionament dels quals es regeixi per l'article 29 de la Llei orgànica 15/1999, de 13 de desembre.

c) Aquells els responsables dels quals siguin administracions tributàries i es relacionin amb l'exercici de les seves potestats tributàries.

d) Aquells els responsables dels quals siguin les entitats financeres per a finalitats relacionades amb la prestació de serveis financers.

e) Aquells els responsables dels quals siguin les entitats gestores i serveis comuns de la Seguretat Social i es relacionin amb l'exercici de les seves competències. De la mateixa manera, aquells els responsables dels quals siguin les mútues d'accidents de treball i malalties professionals de la Seguretat Social.

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.

3. A més de les mesures de nivell bàsic i mitjà, les mesures de nivell alt s'han d'aplicar en els següents fitxers o tractaments de dades de caràcter personal:

a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.

b) Els que continguin o es refereixin a dades obtingudes per a fins policials sense consentiment de les persones afectades.

c) Els que continguin dades derivades d'actes de violència de gènere.

4. Als fitxers els responsables dels quals siguin els operadors que prestin serveis de comunicacions electròniques disponibles al públic o explotin xarxes públiques de comunicacions electròniques respecte a les dades de tràfic i a les dades de localització, s'hi han d'aplicar, a més de les mesures de seguretat de nivell bàsic i mitjà, la mesura de seguretat de nivell alt que conté l'article 103 d'aquest Reglament.

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.

6. També es poden implantar les mesures de seguretat de nivell bàsic en els fitxers o tractaments que continguin dades relatives a la salut, referents exclusivament al grau de discapacitat o la simple declaració de la condició de discapacitat o invalidesa de l'afectat, amb motiu del compliment de deures públics.

7. Les mesures incloses en cadascun dels nivells descrits anteriorment tenen la condició de mínims exigibles, sense perjudici de les disposicions legals o reglamentàries específiques vigents que puguin ser aplicables en cada cas o les que per pròpia iniciativa adopti el responsable del fitxer.

8. Als efectes de facilitar el compliment del que disposa aquest títol, quan en un sistema d'informació hi hagi fitxers o tractaments que, en funció de la seva finalitat o ús concret, o de la naturalesa de les dades que continguin, requereixin l'aplicació d'un nivell de mesures de seguretat diferent que el del sistema principal, es poden segregar d'aquest últim, i és aplicable en cada cas el nivell de mesures de seguretat corresponent i sempre que es puguin delimitar les dades afectades i els usuaris que hi tinguin accés, i que això es faci constar en el document de seguretat.

Situació actual:

A data de la present auditoria l'entitat disposa de tres fitxers inscrits davant del Registre General l'Agència Espanyola de Protecció de Dades: Fitxer de *Personal*, codi d'inscripció número 2042100219; Fitxer de Prevenció *de Riscos Laborals*, codi d'inscripció número 2042100221; i Fitxer d'*Administració*, codi d'inscripció número 20421002020; i d'un fitxer inscrit davant l'Agència Catalana de Protecció de Dades anomenat Col·legiats.

És necessari comentar que els tres primers fitxers són de caràcter privat i per tant subjectes a l'Agència Espanyola de Protecció de Dades, mentre que el de Col·legiats és de naturalesa pública (art.35 de la Llei 7/2006, de 31 de maig, al considerar els col·legis professionals como corporacions de dret públic), és per això que prèvia inscripció al Registre de l'APDCAT es va publicar una disposició de caràcter general de creació del fitxer (DOGC número 4155, de data 16 de juny de 2004).

Atenent a la tipologia de dades que es tracten i d'acord amb el que estipula la normativa, correspon el nivell de seguretat alt als Fitxers de Personal, i de Prevenció de Riscos Laborals, el nivell de seguretat mitjà al Fitxer de Col·legiats i el nivell de seguretat bàsic al Fitxer d'Administració.

No obstant, un cop consultat el registre on-line de la mateixa Agència s'ha pogut constatar que els fitxers no es troben degudament actualitzats. Durant el present any s'ha produït un canvi en la seu de l'entitat, i també del seu domicili social, que ha passat del Carrer Alcoi 21 al Carrer Pujades 350 local, també de Barcelona. A més, actualment consta com un tractament de dades automatitzat quan en realitat també és en paper, per tant seria mixt.

Àrees de millora

L'entitat hauria de fer una revisió dels fitxers que es troben actualment inscrits davant del Registre General de Protecció de Dades de l'AEPD per tal de procedir a l'actualització dels mateixos en base a les necessitats de l'entitat.

En aquest sentit caldria Fer una modificació dels fitxers de Col·legiats, Personal, Prevenció de Riscos Laborals i Administració, per tal d'actualitzar el seu contingut detallant el nou domicili social de l'entitat i adequant el tractament de les dades a la realitat vigent.

6.2. Encarregat/s del tractament

Article 82 RDLOPD.- *1. Quan el responsable del fitxer o tractament faciliti l'accés a les dades, als suports que les contenen o als recursos del sistema d'informació que les tracta, a un encarregat de tractament que presti els seus serveis en els locals del primer, s'ha de fer constar aquesta circumstància en el document de seguretat del dit responsable, i el personal de l'encarregat s'ha de comprometre al compliment de les mesures de seguretat previstes en l'esmentat document.*

Quan aquest accés sigui remot i s'hagi prohibit a l'encarregat incorporar aquestes dades a sistemes o suports diferents dels del responsable, aquest últim ha de fer constar aquesta circumstància en el document de seguretat del responsable, i el personal de l'encarregat s'ha de comprometre al compliment de les mesures de seguretat previstes en l'esmentat document.

2. Si el servei el presta l'encarregat del tractament en els seus propis locals, aliens als del responsable del fitxer, ha d'elaborar un document de seguretat en els termes que exigeix l'article 88 d'aquest Reglament o completar el que ja hagi elaborat, si s'escau, identificant el fitxer o tractament i el seu responsable i incorporant les mesures de seguretat a implantar en relació amb el tractament esmentat.

3. En tot cas, l'accés a les dades per part de l'encarregat del tractament està sotmès a les mesures de seguretat que preveu aquest Reglament.

Situació actual:

Inicialment, cal indicar que s'ha d'entendre com encarregat de tractament a aquell tercer a qui el responsable del fitxer facilita accés a dades de caràcter personal per raó de la prestació d'un servei determinat.

Durant els treballs d'auditoria s'ha pogut detectar que l'entitat disposa de diversos encarregats de tractament:

- L'empresa SOFTENG de gestió i manteniment informàtic.
- L'empresa FAURA-CASAS, AUDITORS-CONSULTORS S.L. per a les tasques d'administració de personal.
- Assessors del COIB sense contracte laboral, tant aquells que presten serveis amb una periodicitat determinada com aquells que només ho fan de forma puntual, com per exemple els assessors de recerca.
- BUFET VALLBÉ per al tractament de casos judicials.
- L'empresa SERVICIOS PLANOS DE MANIPULADOS per a l'enviament de les nòmines als treballadors.

- Una freelance que presta serveis de fotografia.

S'ha pogut acreditar documentalment que amb alguns dels anteriors tercers hi ha signat un compromís de confidencialitat, però amb altres com BUFET VALLBÉ o la freelance no hi ha cap document de protecció de dades signat. A més, hem de tenir en compte que el compromís de confidencialitat esmentat no inclou les disposicions que serien exigibles per a un encarregat de tractament.

Per tant, ha quedat acreditat que no s'ha formalitzat la relació amb tots els tercers oportuns mitjançant un contracte d'encarregat de tractament segons estipula l'article 12 de la LOPD.

Àrees de millora

L'entitat ha de realitzar una tasca de recopilació i control dels contractes signats amb terceres empreses que puguin tenir o tinguin accés a dades de caràcter personal, a fi de revisar-los i en cas que no hagin estat incloses les clàusules oportunes d'encarregat de tractament, fer les gestions oportunes per complir amb aquests extrems el més aviat possible.

En aquest sentit seria necessari abandonar la tendència actual en virtut de la qual tots els tercers signen un compromís de confidencialitat per defecte. En definitiva, si un tercer, tant persona física com jurídica, ha d'accedir a dades personals a compte del COIB per a la prestació d'un servei determinat haurà de signar un contracte d'encarregat de tractament. Si pel contrari no ha de tenir-ne accés però per raó del servei prestat podria accedir a determinada informació, haurà de signar un compromís de confidencialitat, tal i com s'esmenta en el punt 6.3.

Tanmateix, en cas que hi hagués una relació amb intercanvi de dades amb entitats amb les que no hi ha plasmada per escrit la prestació del servei, seria necessari signar un contracte d'encarregat de tractament.

També cal que s'indiqui si el tractament de les dades es fa dins de les instal·lacions del responsable del fitxer o si per contra es realitza integrament fora de les ja esmentades instal·lacions.

Per últim, hem de fer esment a aspectes en els que l'entitat hauria d'incidir:

- A part de plasmar en els contractes les disposicions que estableix l'art.12 LOPD, cal que sempre s'estableixin les mesures de seguretat que haurà de complir l'encarregat per a la prestació del servei determinat.

- L'entitat també ha de vetllar perquè els encarregats de tractament compleixin amb les mesures de seguretat que estableix el RD 172072007. Per això, seria recomanable demanar una certificació a l'encarregat de tractament conforme aquest compleix amb la normativa de protecció de dades, com per exemple

demanant una còpia de l'última auditoria realitzada o un certificat de la realització de la mateixa.

6.3. Prestació de servei sense accés a dades personals

Article 83 RDLOPD.- *El responsable del fitxer o tractament ha d'adoptar les mesures adequades per limitar l'accés del personal a dades personals, als suports que les continguin o als recursos del sistema d'informació, per a la realització de treballs que no impliquin el tractament de dades personals.*

Quan es tracti de personal aliè, el contracte de prestació de serveis ha de recollir expressament la prohibició d'accedir a les dades personals i l'obligació de secret respecte a les dades que el personal hagi pogut conèixer amb motiu de la prestació del servei.

Situació actual:

Un cop realitzat el treball de camp de l'entitat auditada, cal indicar que només hi ha un cas en el que hi hagi empreses externes que presten serveis a l'entitat, però que no tenen accés a dades personals. Concretament hi ha constituïda una comunitat de propietaris a l'edifici i a través d'aquesta es presten una sèrie de serveis, com el de neteja, climatització o seguretat.

No s'ha pogut acreditar documentalment l'existència d'un compromís de confidencialitat amb les empreses que presten els serveis anteriorment esmentats.

De totes maneres, l'entitat manifesta que aquest personal aliè només pot accedir a les ubicacions determinades i en cap cas ha d'accedir a informació que contingui dades de caràcter personal.

Àrees de millora

És preceptiu fer signar a les empreses que presten serveis a compte de l'entitat però que no tenen accés a dades els corresponents compromisos de confidencialitat.

A més a més, cal que en el contracte de prestació de serveis si és que existeix, o en el propi compromís de confidencialitat, es reculli expressament la prohibició d'accedir a les dades personals.

6.4. Delegació d'autoritzacions

Article 84 RDLOPD.- *Les autoritzacions que en aquest títol s'atribueixen al responsable del fitxer o tractament poden ser delegades en les persones designades a aquest efecte. En el document de seguretat hi han de constar les persones habilitades per atorgar aquestes autoritzacions, així com aquelles en les quals recau la delegació esmentada. En cap cas aquesta designació suposa una delegació de la responsabilitat que correspon al responsable del fitxer.*

Situació actual:

En els Document de Seguretat de l'entitat hi consten els càrrecs que actuen com a responsables de seguretat però també els encarregats de certs tràmits en matèria de protecció de dades com per exemple: de la introducció de clàusules de protecció de dades als contractes mercantils és responsabilitat de la Gerència o de persones delegades per aquesta, i de la signatura dels compromisos de confidencialitat és responsable l'Auditor Intern - Responsable de Qualitat.

Per una altra banda, durant els treballs d'auditoria s'ha pogut comprovar que també existeix una Comissió de Qualitat que és responsable de donar suport en temes de protecció de dades.

Àrees de millora

No detectada.

Seria necessari que constés a tots els Documents de Seguretat la figura de la Comissió de Qualitat, així com un detall de les seves funcions i els càrrecs que en formen part.

En definitiva, quan efectivament hi hagi constància que s'ha produït una delegació de funcions del responsable del fitxer en altres responsables, i per tant hi hagi altres persones que vetllin per l'efectiu compliment de les mesures de seguretat en el RD 1720/2007 indicades apart del responsable de seguretat, caldrà que aquesta delegació es faci constar explícitament als Documents de Seguretat de l'entitat.

6.5. Accés a dades a través de xarxes de comunicacions

Article 85 RDLOPD.- *Les mesures de seguretat exigibles als accessos a dades de caràcter personal a través de xarxes de comunicacions, siguin públiques o no, han de garantir un*

nivell de seguretat equivalent al corresponent als accessos en mode local, conforme als criteris que estableix l'article 80.

Situació actual:

Com a previ és necessari comentar que l'entitat durant l'any 2009 va tenir una auditoria de seguretat informàtica realitzada per una empresa externa i els resultats varen ser satisfactoris.

Les mesures que es prenen a nivell de seguretat informàtica són gestionades i controlades pels tècnics de l'empresa SOFTENG. No obstant, les dades de l'entitat es guarden als servidors del COIB, mai a les dependències de SOFTENG.

A nivell de seguretat lògica tot el software amb el que es treballa és de MICROSOFT. Tot el que entra i surt de l'entitat, ja sigui via e-mail, Internet, etc, es controla per un firewall de protecció perimetral que fa de proxy. També es treballa amb l'antivirus de l'empresa PANDA que també inclou antispam, antimalware, etc. Per tant, queda clar que hi ha un doble filtratge, i a més amb dos fabricants diferents.

Tots els usuaris tenen accés a Internet, però també és cert que hi ha determinats filtres per categories de pàgines web. Pel que fa al correu electrònic també en té tothom, fins i tot els assessors.

En principi tota la informació generada hauria d'estar al servidor. En aquest sentit s'informa als usuaris de la necessitat que al disc dur local del seu ordinador no es guardi informació de l'entitat.

Tots els equips disposen de WINDOWS 7 i de MICROSOFT OFFICE.

A nivell de programari, es treballa amb un programa propi per a la gestió col·legial anomenat ULISSES. Per a la comptabilitat es treballa amb el CONTAPLUS. També es treballa amb dos programes més però que a data de la present auditoria no tracten dades personals, es tracta de l'IMMAGIC per a la gestió de la biblioteca i de documents, i amb el programa A3 que en un futur serà emprat per l'entitat per a la gestió de recursos humans.

Podem afirmar que els accessos a dades a través de xarxes de comunicacions garanteixen un nivell de seguretat equivalent als accessos en mode local.

Àrees de millora

No detectada.

6.6. Règim de treball fora dels locals de la ubicació dels fitxers

Article 86 RDLOPD.- *1. Quan les dades personals s'emmagatzemin en dispositius portàtils o es tractin fora dels locals del responsable de fitxer o tractament, o de l'encarregat del tractament, és necessari que hi hagi una autorització prèvia del responsable del fitxer o tractament, i en tot cas s'ha de garantir el nivell de seguretat corresponent al tipus de fitxer tractat.*

2. L'autorització a què es refereix el paràgraf anterior ha de constar en el document de seguretat i es pot establir per a un usuari o per a un perfil d'usuaris i se n'ha de determinar un període de validesa.

Situació actual:

Tot i que el règim de treball està pensat per al tractament de les dades de caràcter personal des dels locals on es troben ubicats els fitxers, també es produeixen accessos remots a dades personals.

Concretament ens trobem davant de dos casos: en primer lloc és el cas dels tècnics de SOFTENG que en la seva figura d'administrador del sistema bàsicament accedeixen remotament al sistema per a la gestió i manteniment dels servidors. També tenen aquest accés alguns usuaris, com per exemple el gerent de l'entitat, que prèviament ho hagin comunicat als tècnics de SOFTENG.

De totes maneres, les mesures de seguretat emprades són les mateixes en ambdós casos. Tot usuari ha d'accedir mitjançant un nom d'usuari i una contrasenya, i l'accés és via Terminal Server i la comunicació és encriptada. A més, hi ha un firewall que controla aquests accessos.

A més, en el cas de SOFTENG l'accés només es pot realitzar a través de la seva IP pública, és a dir, només dins de les seves instal·lacions.

Es pot afirmar per tant que les mesures de seguretat emprades per al treball fora del lloc on s'ubiquen els fitxers són les adequades.

Per últim, esmentar que tots els usuaris de l'entitat poden accedir al seu correu electrònic via webmail.

Àrees de millora

A diferència del que succeeix actualment cal que el responsable del fitxer inclogui dins del document de seguretat corresponent, o en un document annex, la relació d'usuaris o entitats que estan autoritzats a accedir remotament a les dades, tant si és per un usuari concret com per un perfil d'usuaris.

S'haurà de constar en el document de seguretat aquesta autorització per part del responsable del fitxer, així com determinar un període de validesa per a la mateixa. També seria bo adjuntar un protocol que ho detalli.

6.7. Fitxers temporals

Article 87 RDLOPD.- *1. Els fitxers temporals o còpies de documents que s'han creat exclusivament per a la realització de treballs temporals o auxiliars han de complir el nivell de seguretat que els correspongui conforme als criteris establerts a l'article 81.*

2. Qualsevol fitxer temporal o còpia de treball creat així s'ha d'esborrar o destruir una vegada deixi de ser necessari per als fins que van motivar la seva creació.

Situació actual:

La veritat és que cada és menys habitual que es generin fitxers temporals amb dades de caràcter personal, donat que a dia d'avui els programes emprats ja satisfan quasi totes les necessitats existents.

No obstant, el mateix programa ULISSES permet fer extraccions de dades en arxius ofimàtics, com en Word. Hi ha una carpeta al servidor que custodia les plantilles en Word, i si l'usuari després ho desitja pot guardar el document al servidor un cop introduïdes les dades, també al servidor.

Si bé és cert que no es porta cap control informàtic de la creació i permanència d'aquest tipus de fitxers, l'entitat manifesta que aquest control seria factible de realitzar.

Àrees de millora

Sabem que és inherent a qualsevol organització la generació de fitxers ofimàtics paral·lels amb dades de caràcter personal, ara bé, és necessari conscienciar als àmbits més proclius a generar fitxers, de la transcendència d'eliminar-los un cop ha finalitzat el seu ús.

Per això, tot i que en el cas de l'entitat objecte d'auditoria els casos serien reduïts, caldria fer recordatoris periòdics, com per exemple per circular via e-mail, per tal de conscienciar als usuaris de la necessitat de la necessitat d'eliminar els fitxers temporals amb dades personals un cop ja no resulten necessaris, incloent la prohibició de guardar fitxers amb dades de caràcter personal en el disc dur local dels ordinadors. A més, entenem que caldria fer entrega d'un Manual de Bones Pràctiques que inclogués disposicions en relació als fitxers temporals.

6.8. Document de seguretat

Article 88 RDLOPD.- *1. El responsable del fitxer o tractament ha d'elaborar un document de seguretat que reculli les mesures d'índole tècnica i organitzativa conformes amb la normativa de seguretat vigent que és de compliment obligat per al personal amb accés als sistemes d'informació.*

2. El document de seguretat pot ser únic i ha d'incloure tots els fitxers o tractaments, o bé individualitzat per a cada fitxer o tractament. També es poden elaborar diferents documents de seguretat agrupant fitxers o tractaments segons el sistema de tractament utilitzat per a la seva organització, o bé atenent criteris organitzatius del responsable. En tot cas té el caràcter de document intern de l'organització.

3. El document ha de contenir, com a mínim, els aspectes següents:

a) Àmbit d'aplicació del document amb especificació detallada dels recursos protegits.

b) Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit en aquest Reglament.

c) Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers.

d) Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten.

e) Procediment de notificació, gestió i resposta davant les incidències.

f) Els procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats.

g) Les mesures que sigui necessari adoptar per al transport de suports i documents, així com per a la destrucció dels documents i suports o, si s'escau, la reutilització d'aquests últims.

4. En cas que siguin aplicables als fitxers les mesures de seguretat de nivell mitjà o les mesures de seguretat de nivell alt, previstes en aquest títol, el document de seguretat ha de contenir a més:

a) La identificació del responsable o responsables de seguretat.

b) Els controls periòdics que s'han de realitzar per verificar el compliment del que disposa el document.

5. Quan hi hagi un tractament de dades per compte de tercers, el document de seguretat ha de contenir la identificació dels fitxers o tractaments que es tractin en concepte d'encarregat amb referència expressa al contracte o document que reguli les condicions de l'encàrrec, així com la identificació del responsable i del període de vigència de l'encàrrec.

6. En els casos en què dades personals d'un fitxer o tractament s'incorporin i es tractin de manera exclusiva en els sistemes de l'encarregat, el responsable ho ha d'anotar en el seu document de seguretat. Quan aquesta circumstància afecti una part o la totalitat dels fitxers o tractaments del responsable, es pot delegar en l'encarregat l'administració del document de seguretat, excepte pel que fa a les dades incloses en recursos propis. Aquest fet s'ha d'indicar de manera expressa en el contracte subscrit a l'empara de l'article 12 de la Llei orgànica 15/1999, de 13 de desembre, amb especificació dels fitxers o tractaments afectats.

En aquest cas, cal atenir-se al document de seguretat de l'encarregat a l'efecte del compliment del que disposa aquest Reglament.

7. El document de seguretat s'ha de mantenir actualitzat en tot moment i s'ha de revisar sempre que es produeixin canvis rellevants en el sistema d'informació, en el sistema de tractament que es fa servir, en la seva organització, en el contingut de la informació inclosa en els fitxers o tractaments o, si s'escau, com a conseqüència dels controls periòdics realitzats. En tot cas, s'entén que un canvi és rellevant quan pot repercutir en el compliment de les mesures de seguretat implantades.

8. El contingut del document de seguretat sempre s'ha d'adequar a les disposicions vigents en matèria de seguretat de les dades de caràcter personal.

Article 95 RDLOPD.- *En el document de seguretat s'han d'assignar un o diversos responsables de seguretat encarregats de coordinar i controlar les mesures que hi estan definides. Aquesta designació pot ser única per a tots els fitxers o tractaments de dades de caràcter personal o diferenciada segons els sistemes de tractament utilitzats, circumstància que s'ha de fer constar clarament en el document de seguretat.*

En cap cas aquesta designació suposa una exoneració de la responsabilitat que correspon al responsable del fitxer o a l'encarregat del tractament d'acord amb aquest Reglament.

Article 105 RDLOPD.- *1. A més del que disposa el present capítol, als fitxers no automatitzats els és aplicable el que disposen els capítols I i II del present títol pel que fa a:*

a) Abast.

b) Nivells de seguretat.

c) Encarregat del tractament.

d) Prestacions de serveis sense accés a dades personals.

e) Delegació d'autoritzacions.

f) Règim de treball fora dels locals del responsable del fitxer o encarregat del tractament.

g) Còpies de treball de documents.

h) Document de seguretat.

2. Així mateix se'ls ha d'aplicar el que estableix la secció primera del capítol III del present títol pel que fa a:

a) Funcions i obligacions del personal.

b) Registre d'incidències.

c) Control d'accés.

d) Gestió de suports.

Article 109 RDLOPD.- *S'han de designar un o diversos responsables de seguretat en els termes i amb les funcions que preveu l'article 95 d'aquest Reglament.*

Situació actual:

L'entitat disposa d'un Document de Seguretat per a cadascun dels quatre fitxers que es troben actualment inscrits. En tot cas aquests documents es troben en la seva segona versió de maig de 2010.

Si bé és cert que l'entitat ha fet un esforç per tal d'adequar plenament el Documents de Seguretat als requeriments que estableix la normativa de protecció de dades, la veritat és que aquests no reflecteixen la realitat actual de l'entitat en la matèria ni es troben degudament actualitzats.

A mes a més estan construïts en base al RD 994/1999, norma que ja va ser derogada per l'actual RD 1720/2007, en vigor des del passat 18 d'abril de 2008.

Tanmateix, al DS d'Administració hi consta un nivell de seguretat alt, quan en realitat per les dades que hi consten al document el nivell de seguretat hauria de ser bàsic.

També és important comentar respecte el DS de Col·legiats el següent:

- El nom del DS és Col·legiades, quan en realitat el fitxer s'anomena Col·legiats.

- A cadascun dels Documents de Seguretat de nivell mitjà i alt hi consten els responsables de seguretat, però en el de Col·legiats surt com a tal el responsable d'informàtica i el responsable d'administració, càrrecs que durant els treballs d'auditoria no existien dins de l'entitat.

Una altra mancança important radica en el fet que en cap dels Documents de Seguretat hi apareix un apartat que esmenti les mesures que es prenen tant quan un suport informàtic i/o en paper ha de ser reutilitzat o rebutjat.

A més, a continuació esmentem altres aspectes:

- Procediment mitjançant el qual s'assignen, distribueixen i emmagatzemen les contrasenyes.
- Pel que fa a les funcions i obligacions, podem dir que estan definides de manera general remetent-se a que els usuaris firmen un document anomenat "Full d'Informació i Compromís de la Treballadora".
- Tampoc es referencia el llistat persones físiques o jurídiques que realitzen una prestació com a encarregats de tractament.
- La resta d'apartats que es contemplen als altres punts de l'informe.

Àrees de millora

Cal que els Documents de Seguretat continguin totes les directrius establertes pel RD 1720/2007 de 21 de desembre, tant pel que respecta a les mesures en suports automatitzats com no automatitzats, desenvolupant cadascun dels quatre fitxers esmentats. Aquest aspecte pren encara més transcendència amb el canvi de reglament de mesures de seguretat, pel que s'hauran de corregir les referències a la normativa ja derogada.

Tanmateix, hauran de trobar-se actualitzats en tot moment i descriure la realitat de l'entitat, incorporant la descripció dels apartats legalment requerits, així com tots els protocols relatius a confidencialitat i mesures de seguretat que tinguin incidència en els fitxers.

En aquest sentit, cal incloure les modificacions apuntades en el punt de "Situació actual" que, entre d'altres, suposa la modificació del nivell de seguretat del DS d'Administració i els apunts en relació al DS de Col·legiats.

6.9. Funcions i obligacions del personal

Article 89 RDLOPD.- *1. 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 han d'estar clarament definides i documentades en el document de seguretat.*

També s'han de definir les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament.

2. El responsable del fitxer o tractament ha d'adoptar les mesures necessàries perquè el personal conegui d'una forma comprensible les normes de seguretat que afectin l'exercici de les seves funcions així com les conseqüències en què pugui incórrer en cas d'incompliment.

Situació actual:

A l'apartat 4 dels Documents de Seguretat de l'entitat s'estableix que el seu contingut és d'obligat compliment per a tots els treballadors i que el responsable del fitxer ha de vetllar perquè tothom que pugui tenir accés a dades personals tingui coneixement de l'existència d'aquest document. Posteriorment en els mateixos s'informa d'una sèrie de drets i obligacions de tipus genèric, entre d'altres la obligatorietat de mantenir la confidencialitat i a sotmetre's a les mesures de seguretat que determina el responsable del fitxer.

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 estan definides operativament, no es troben documentades en el Document de Seguretat. Únicament als DS, amb l'excepció del DS de Col·legiats, hi ha un quadre amb el llistat de les persones usuàries de les dades compreses dins del fitxer.

A cada nova incorporació laboral se li fa signar un document anomenat "Informació i Compromís de la Treballadora" a través del qual es compleix amb el deure d'informació previst a l'art.5 LOPD i en el que la signant es compromet a mantenir el secret professional. Per la seva banda, els assessors signen un compromís de confidencialitat.

Si bé és cert que no es fan sessions específiques en matèria de protecció de dades, a nivell informàtic se li explica a l'usuari verbalment en el moment de la seva incorporació quina és la política de seguretat, contrasenyes, salvapantalles, etc, i segons la situació es podrien fer recordatoris específics.

Per últim, tan sols esmentar que durant els treballs de camp de l'entitat auditada es va poder detectar que els usuaris de l'entitat han pres consciència dels drets i obligacions que suposa la normativa de protecció de dades, i el seu nivell de coneixement és ascendent.

Àrees de millora

No detectada.

Tot i així, les funcions i obligacions dels usuaris o perfils d'usuaris amb accés a dades personals haurien de quedar relacionades als corresponents Documents de Deguretat.

Aquesta instrucció és per a tots els usuaris de l'entitat, ja sigui personal laboral com els assessors. En aquest s'hi haurien de plasmar mesures a tenir en compte en el tractament de la informació, com per exemple les de tipus informàtic.

Com ja hem comentat a l'apartat 6.2 del present informe els anomenats assessors es consideren com encarregats de tractament. A data de la present auditoria aquests persones signen un compromís de confidencialitat, pel que caldria modificar aquesta política i fer que signessin un contracte d'encarregat de tractament. En canvi, si s'acaba fent entrega del Manual de Bones Pràctiques esmentat, pel fet que aquests assessors presten serveis dins de les dependències de l'entitat seria necessari que també se'ls fes entrega de l'esmentat document.

6.10. Registre d'incidències

Article 90 RDLOPD.- *Hi ha d'haver un procediment de notificació i gestió de les incidències que afectin les dades de caràcter personal i s'ha d'establir un registre en què es faci constar el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes que se'n deriven i les mesures correctores aplicades.*

Article 100 RDLOPD.- *1. En el registre que regula l'article 90 s'hi han de consignar, a més, els procediments de recuperació de les dades realitzats, i s'hi han d'indicar la persona que va executar el procés, les dades restaurades i, si s'escau, quines dades ha estat necessari gravar manualment en el procés de recuperació.*

2. És necessària l'autorització del responsable del fitxer per a l'execució dels procediments de recuperació de les dades.

Situació actual:

A cadascun dels Documents de Seguretat s'explicita tot el referent al registre d'incidències. L'entitat entén com a incidència qualsevol fet que pugui suposar un perill per a la seguretat del fitxer, des dels punts de vista de confidencialitat, integritat o disponibilitat.

Actualment és important diferenciar si la incidència és informàtica o no donat que la via de tractament i resolució és diferent. De totes maneres, en ambdós casos és l'usuari que la detecta el responsable de comunicar-la a la persona que procedirà a la seva resolució, com a continuació explicarem.

Quan es tracta d'una incidència informàtica, l'usuari ha de contactar amb una administrativa concreta de l'entitat que l'anota en un arxiu Excel destinat a tal efecte, i si no la pot resoldre ella mateixa, la notifica a un dels tècnics informàtics de l'empresa SOFTENG, prioritzant en tot cas les tasques a dur a terme. Aquest tècnic la gestiona i resol.

Un cop resolta la incidència s'anota a l'Excel esmentat i es notifica la seva resolució a l'usuari. Aquest arxiu diferencia les tasques que realitza tant el tècnic informàtic com la pròpia administrativa esmentada. El tècnic informàtic de SOFTENG a l'arribar a les dependències de la seva empresa envia un report a l'administrativa de les tasques realitzades durant el dia, i en el seu sistema d'imputació d'hores diàries també es registra la incidència.

No s'ha pogut acreditar si l'arxiu Excel comentat contempla tots els camps exigibles en el cas que la incidència tingués afectació a dades de caràcter personal. En canvi, en el sistema d'imputació d'hores diàries de SOFTENG es recull el número d'incidència, la data d'incidència, la data de comunicació, la prioritat, l'usuari que la detecta, i la descripció de la mateixa.

Es manifesta que a nivell informàtic s'han anotat totes les incidències produïdes, i en aquest sentit s'inclouen efectivament els procediments de recuperació de dades.

Per una altra banda tenim el registre de les incidències no informàtiques, com per exemple algunes anotades recentment en relació al trasllat de la documentació des de les anteriors instal·lacions del Carrer Alcoi a les actuals. En aquest cas el procediment és més senzill, quan l'usuari la detecta li ho comunica a Gerència o a l'Auditor Intern, i aquest últim la registra en un document destinat a tal efecte i s'encarrega de la seva correcta resolució. D'aquestes incidències es genera un llistat anual que s'actualitza cada mes.

En aquest registre s'hi contenen els requeriments legalment exigibles: tipus i codi d'incidència, departament o secció on s'ha produït, descripció i data de la mateixa, treballador que la detecta i responsable de l'àrea o departament afectat, solució presa, responsable de la solució, resultat de l'acció presa i data de tancament.

Tant un registre com l'altre es revisen periòdicament fins que no es tanca la incidència.

Àrees de millora

En relació a les incidències informàtiques caldria revisar si l'arxiu Excel esmentat recull tots els paràmetres exigibles reglamentàriament, és a dir, el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes que se'n deriven i les mesures correctores aplicades. Una altra opció seria sol·licitar una còpia a SOFTENG de les

incidències produïdes i d'aquelles que tinguin afectació en matèria de protecció de dades afegir els camps que s'escaiguin.

Hem de tenir en compte també que per a les incidències informàtiques produïdes amb dades de nivell mig, en aquest cas segurament serien les que tinguin a veure amb les dades dels col·legiats, cal consignar a més en el registre d'incidències els procediments de recuperació de les dades realitzats, i s'hi han d'indicar la persona que va executar el procés, les dades restaurades i, si s'escau, quines dades ha estat necessari gravar manualment en el procés de recuperació.

Tanmateix i d'aplicació a ambdós registres, a efectes de poder acreditar el moment en el que s'ha produït la incidència seria recomanable registrar també l'hora.

Seria adient fer comunicacions generals periòdiques a tots els usuaris de l'entitat informant de la necessitat de comunicar totes les incidències que es produeixen en matèria de protecció de dades.

Per últim, esmentar que als Documents de Seguretat s'hi hauria de registrar el procediment que es segueix per a la gestió i resolució de les incidències informàtiques, donat que el contingut a data de la present revisió respon més aviat al tractament de les no informàtiques.

6.11. Control d'accés

Article 91.- *1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.*

2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.

3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.

4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.

5. En cas que hi hagi personal aliè al responsable del fitxer que tingui accés als recursos, ha d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi.

Article 99 RDLOPD.- *Exclusivament el personal autoritzat en el document de seguretat pot tenir accés als llocs on estiguin instal·lats els equips físics que donin suport als sistemes d'informació.*

Article 111 RDLOPD.- *1. Els armaris, arxivadors o altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal han d'estar en àrees en què l'accés estigui protegit amb portes d'accés dotades de sistemes d'obertura mitjançant una clau o un altre dispositiu equivalent. Aquestes àrees s'han de mantenir tancades quan no sigui necessari l'accés als documents inclosos en el fitxer.*

2. Si, ateses les característiques dels locals de què disposa el responsable del fitxer o tractament, no és possible complir el que estableix l'apartat anterior, el responsable ha

d'adoptar mesures alternatives que, degudament motivades, s'han d'incloure en el document de seguretat.

Article 113 RDLOPD.- *1. L'accés a la documentació s'ha de limitar exclusivament al personal autoritzat.*

2. S'han d'establir mecanismes que permetin identificar els accessos realitzats en el cas de documents que puguin ser utilitzats per múltiples usuaris.

3. L'accés de persones no incloses en el paràgraf anterior ha de quedar adequadament registrat d'acord amb el procediment establert a aquest efecte en el document de seguretat.

Situació actual:

Accés Lògic:

Els usuaris només poden accedir a les dades i recursos que necessiten per al desenvolupament de les seves funcions. Els mecanismes que impedeixen que els usuaris accedeixin a més dades de les autoritzades seria l'ús de contrasenyes.

Hi ha tres subgrups a tenir en compte a nivell de perfil d'usuari, un per recursos, un per usuaris i un altre per grups de seguretat. El referent a recursos és a nivell de hardware, els grups de seguretat van per usuaris específics i se'ls assigna un perfil determinat, mentre que els usuaris estan dividits per organigrama d'empresa dividits per departaments.

L'entitat manifesta que no hi ha cap carpeta o programa sense una política de perfils detallada. Un exemple important d'aquesta política de perfils la trobem en el cas de la informació generada per l'anomenat "Programa Retorn", informació que es custodia en una carpeta del servidor i que per la seva especial sensibilitat només hi ha de tenir accés la persona encarregada del servei, com succeeix en realitat.

Hi ha la possibilitat d'extreure de forma automatitzada i del tot actualitzada una relació d'usuaris a través de l'Active Directory. Aquesta relació inclou també els perfils d'aquests.

Per a l'alta d'un nou usuari és el responsable del departament en qüestió qui ho ha de comunicar per e-mail al tècnic informàtic de SOFTENG o també pot ser que consti com una de les tasques a realitzar a través de l'administrativa encarregada. El tècnic és l'encarregat de donar d'alta a l'usuari al sistema i llavors comunica el nom d'usuari i la contrasenya (genèrica) al responsable del departament, que a la seva vegada és el responsable de comunicar-li a l'usuari. La contrasenya ha de ser canviada al primer accés.

Tant la modificació com la baixa d'un usuari funcionen seguint el mateix procediment. En el cas de la baixa els tècnics de SOFTENG no eliminen directament

l'usuari, es deshabilita, però passat un mes sense reincorporació de l'usuari sí que s'eliminaria.

El personal aliè que treballa a l'entitat està sotmès a les mateixes regles a nivell informàtic que el personal propi. Aquest seria el cas dels assessors.

Accés físic:

Cal indicar que un cop revisades les instal·lacions s'ha pogut comprovar que per accedir a les dependències de l'entitat i a les dependències en les que es guarden dades personals sempre es requereix de targeta o bé de clau.

Pel que fa al CPD, aquest està ubicat a la primera planta del centre. Es necessita una clau per accedir a la sala de servidors i una altra clau per accedir al CPD. Les claus les custodia únicament l'administrativa encarregada de certes funcions informàtiques, la resta de persones que hi vulguin accedir li ho han de demanar expressament. El personal de manteniment pot accedir a la sala de servidors però no al CPD.

Encara no es registren les entrades i sortides del servidor com es feia quan el CPD estava al Carrer Alcoi, però hi ha previst implantar-ho properament. Les mesures d'alimentació i climatització del CPD són les adequades. Es fan gràfiques de la temperatura, processador i alimentació.

Àrees de millora

No detectada.

Seria necessari que s'inclogués als Documents de Seguretat el llistat de persones autoritzades per accedir al CPD.

6.12. Gestió de suports i documents

Article 92 RDLOPD.- *1. Els suports i documents que continguin dades de caràcter personal han de permetre identificar el tipus d'informació que contenen, han de ser inventariats i només hi ha de poder accedir el personal autoritzat per fer-ho en el document de seguretat.*

S'exceptuen aquestes obligacions quan les característiques físiques del suport impossibilitin el seu compliment, i n'ha de quedar constància motivada en el document de seguretat.

2. La sortida de suports i documents que continguin dades de caràcter personal, inclosos els compresos i/o annexos a un correu electrònic, fora dels locals sota el control del responsable del fitxer o tractament, l'ha d'autoritzar el responsable del fitxer o ha d'estar degudament autoritzada en el document de seguretat.

3. En el trasllat de la documentació s'han d'adoptar les mesures dirigides a evitar la sostracció o pèrdua de la informació o l'accés indegut a aquesta durant el seu transport.

4. Sempre que s'hagi de rebutjar qualsevol document o suport que contingui dades de caràcter personal, s'ha de destruir o esborrar mitjançant l'adopció de mesures dirigides a evitar l'accés a la informació que conté o la seva recuperació posterior.

5. La identificació dels suports que continguin dades de caràcter personal que l'organització consideri especialment sensibles es pot realitzar utilitzant sistemes d'etiquetatge comprensibles i amb significat que permetin als usuaris amb accés autoritzat als suports i documents esmentats identificar el seu contingut, i que en dificultin la identificació per a la resta de persones.

Article 97 RDLOPD.- *1. S'ha d'establir un sistema de registre d'entrada de suports que permeti, directament o indirectament, conèixer el tipus de document o suport, la data i hora, l'emissor, el nombre de documents o suports inclosos en l'enviament, el tipus d'informació que contenen, la forma d'enviament i la persona responsable de la recepció, que ha d'estar degudament autoritzada.*

2. Igualment s'ha de disposar d'un sistema de registre de sortida de suports que permeti, directament o indirectament, conèixer el tipus de document o suport, la data i hora, el destinatari, el nombre de documents o suports inclosos en l'enviament, el tipus d'informació que contenen, la forma d'enviament i la persona responsable del lliurament, que ha d'estar degudament autoritzada.

Article 101 RDLOPD.- *1. La identificació dels suports s'ha de realitzar utilitzant sistemes d'etiquetatge comprensibles i amb significat, que permetin als usuaris amb accés autoritzat als suports i documents esmentats identificar el seu contingut, i que dificultin la identificació per a la resta de persones.*

2. La distribució dels suports que continguin dades de caràcter personal s'ha de fer xifrant les dades esmentades o bé utilitzant un altre mecanisme que garanteixi que la dita informació no sigui accessible o manipulada durant el seu transport.

Així mateix, s'han de xifrar les dades que continguin els dispositius portàtils quan aquests dispositius estiguin fora de les instal·lacions que estan sota el control del responsable del fitxer.

3. S'ha d'evitar el tractament de dades de caràcter personal en dispositius portàtils que no permetin el xifratge. En cas que sigui estrictament necessari, s'ha de fer constar motivadament en el document de seguretat i s'han d'adoptar mesures que tinguin en compte els riscos de realitzar tractaments en entorns desprotegits.

Article 107 RDLOPD.- *Els dispositius d'emmagatzematge dels documents que continguin dades de caràcter personal han de disposar de mecanismes que n'obstaculitzin l'obertura. Quan les característiques físiques d'aquests no permetin adoptar aquesta mesura, el responsable del fitxer o tractament ha d'adoptar mesures que impedeixin que hi puguin accedir persones no autoritzades.*

Article 114 RDLOPD.- *Sempre que es procedeixi al trasllat físic de la documentació que conté un fitxer, s'han d'adoptar mesures dirigides a impedir l'accés a la informació objecte de trasllat o la seva manipulació.*

Situació actual:

Indicar que l'entitat utilitza suports, tant informàtics com en suport paper, que emmagatzemen dades de caràcter personal.

Hi ha un inventari de tots els dispositius de tipus informàtic, dels servidors i de tot el hardware en general. Aquest inventari està plasmat en un arxiu Excel que recull el model, marca, número de sèrie i dades de garantia del dispositiu. Aquest arxiu s'actualitza quan hi ha una alta o una baixa de material.

Tots els dispositius de tipus informàtic són de la marca DELL i disposen d'una etiqueta que inclou el nom i un codi únic que ve de fàbrica.

Les operacions de manteniment i reparació dels suports informàtics sempre es fan internament, no surten mai fora de les instal·lacions de l'entitat. Els suports tenen garantia de DELL, per això són els tècnics d'aquesta empresa els que fan les gestions oportunes a les pròpies ubicacions del COIB.

Els dispositius via USB són suports informàtics que podrien contenir dades personals i sortir fora de les instal·lacions de l'entitat, no estan xifrats. Ara bé, en tot cas es tractaria de dispositius personals dels usuaris, no de tipus corporatiu, però també és cert que no hi ha limitacions ni normes d'ús al respecte.

L'entitat disposa d'un registre d'entrades i sortides en el que recull les entrades i sortides d'informació, CD's i encara que no sigui exigible els e-mails, que contenen dades personals de nivell mig, dades de col·legiats. Aquest registre recull els següents paràmetres: tipus de suport, data i hora d'entrada tot i que per la documentació aportada no s'anota mai l'hora, el receptor, el contingut i els motius.

Pel que fa a la destrucció de suports, en primer lloc i pel que fa als de tipus informàtic es sol formatar el disc dur i amb una aplicació s'omple de nou i aleshores es torna a formatar, procediment que ja no permet recuperar la informació.

Per la seva banda, es disposa d'una màquina trituradora per a la destrucció del paper. No obstant, des del Departament de Formació es manifesta que en alguna ocasió el paper es destrueix a mà.

Àrees de millora

El registre d'entrades i sortides hauria de contenir sempre l'hora, l'emissor i el destinatari, i la forma d'enviament.

Seria necessari que l'entitat informés i recordés a tots els seus usuaris de la necessitat de destruir el paper amb la màquina que hi ha destinada a tal efecte, i no a mà com succeeix amb el Departament de Formació. Si amb la destructora que hi ha no és suficient, caldria adquirir-ne de noves o establir un sistema alternatiu.

Per últim, a continuació presentem una sèrie d'instruccions amb l'objectiu que l'entitat tingui clares quines són les mesures que s'haurien de prendre en el cas que hi hagués constància que s'empren dispositius portàtils amb dades de caràcter personal. Aquestes mesures tenen l'objectiu d'evitar pèrdues d'informació i accessos no autoritzats a dades personals a causa d'un mal ús d'aquest tipus de dispositius, com els USB's:

- Està clar que aquest tipus de dispositius seran utilitzats única i exclusivament amb la finalitat de la prestació dels serveis i tasques pròpies del centre, garantint el compromís de confidencialitat i ètica professional.

- Els dispositius portàtils que tinguin dades personals confidencials hauran d'estar clarament identificats, a través d'un codi per exemple, mitjançant el qual es pugui saber quines són les dades contingudes en el mateix i la data en la qual van ser guardats.

- En el cas que resulti necessari utilitzar aquest tipus de suports, el responsable del fitxer donarà instruccions al responsable de l'àrea corresponent perquè sigui l'encarregat d'autoritzar la idoneïtat del seu ús en cada cas i de controlar les entrades i sortides dels mateixos.

- Aquests moviments dels dispositius sempre que continguin dades de nivell mig, per exemple de col·legiats, hauran de quedar anotats en el registre d'entrades i sortides de suports. En tot cas, les entrades i sortides que s'hagin de fer s'hauran de deixar constància als Document de Seguretat.

- A més, els dispositius d'emmagatzematge dels documents que continguin dades de caràcter personal hauran de disposar de mecanismes que obstaculitzin la seva obertura. Quan les característiques físiques no permetin adoptar aquesta mesura, el responsable del fitxer o tractament adoptarà mesures que impedeixin l'accés de persones no autoritzades.

En la mateixa línea, en cas que els suports que continguin dades de caràcter personal hagin de sortir fora del centre, com per exemple per operacions de manteniment, s'haurà de fer xifrant les dades o bé utilitzant qualsevol altre mecanisme que garanteixi que aquesta informació no sigui intel·ligible ni manipulada durant el transport, ni durant les pròpies operacions.

6.13. Identificació i autenticació d'usuaris

Article 93 RDLOPD.- *1. El responsable del fitxer o tractament ha d'adoptar les mesures que garanteixin la correcta identificació i autenticació dels usuaris.*

2. El responsable del fitxer o tractament ha d'establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de qualsevol usuari que intenti accedir al sistema d'informació i la verificació conforme està autoritzat.

3. Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la confidencialitat i integritat.

4. El document de seguretat ha d'establir la periodicitat, que en cap cas ha de ser superior a un any, amb què s'han de canviar les contrasenyes que, mentre estiguin vigents, s'han d'emmagatzemar de forma inintel·ligible.

Article 98 RDLOPD.- *El responsable del fitxer o tractament ha d'establir un mecanisme que limiti la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació.*

Situació actual:

Als Documents de Seguretat s'estableixen una sèrie de mesures a nivell d'identificació i autenticació dels usuaris, però aquestes no són les que es segueixen a data de la present auditoria.

L'accés dels usuaris ve regulat per un mecanisme a través de l'ús de contrasenyes, fet que permetria identificar a cada usuari de forma inequívoca i personalitzada. Hi ha un doble filtre, un d'accés al sistema i un altre d'accés a l'aplicatiu que correspongui.

Per a l'accés al sistema es requereix d'un nom d'usuari que es correspon amb la inicial del nom i el primer cognom, mentre que la contrasenya ha de tenir un mínim de 6 caràcters, sense un màxim establert ni altres condicionants. Aquestes contrasenyes a data de la present auditoria no caduquen, encara que també és cert que l'usuari se la podria canviar quan ho desitgés.

Per una altra banda, per a l'accés al programa de gestió col·legial s'empra el mateix nom d'usuari que per l'accés al sistema, amb l'excepció d'alguns usuaris més antics amb altres paràmetres. En aquest cas la contrasenya també ha de tenir un mínim de 6 caràcters i tampoc caduca. De totes maneres l'entitat manifesta la seva voluntat de modificar aquesta política i fer que les contrasenyes caduquin cada 4 mesos i que no es pugui posar la mateixa durant 2 anys.

En relació al programa CONTAPLUS, al qual hi tenen accés només 4 persones de l'entitat, el nom d'usuari és el que personalment estableixi el propi usuari, mentre que la contrasenya en aquest cas sí que caduca, concretament cada 45 dies.

Tant en el cas de l'accés al sistema com a CONTAPLUS es limita el número d'intents d'accés no autoritzat, concretament a 3 en ambdós casos. Un cop bloquejada la sessió només un usuari amb permisos d'administrador sobre la gestió d'usuaris, en aquest cas els tècnis informàtics de SOFTENG, pot procedir al seu desbloqueig.

En tot cas les contrasenyes es guarden de forma inintel·ligible mentre estan en vigor, es troben xifrades. Per tant, l'usuari és l'única persona que coneix la seva contrasenya.

En cas d'inactivitat durant un temps determinat el sistema no està preparat perquè es requereixi a l'usuari a tornar a validar-se, fet que podria permetre accessos no autoritzats.

Àrees de millora

És necessari que o bé la contrasenya d'accés al sistema o bé la de cadascuna dels programes que tracten dades de caràcter personal caduqui com a mínim un cop l'any.

El procediment d'identificació i autenticació actualitzat i personalitzat per a cada usuari que accedeixi i/o tracti dades de caràcter personal hauria de ser establert al Document de Seguretat, o en un document annex.

Tot i que no és una mesura legalment exigible, sempre es recomana que en cas d'inactivitat durant un temps determinat, per exemple 10 minuts, es cancel·li la sessió de l'usuari i aquest s'hagi de tornar a validar. És una mesura que té com a objectiu evitar que es produeixin accessos no autoritzats.

6.14. Còpies de recolzament i recuperació

Article 94 RDLOPD.- *1. S'han d'establir procediments d'actuació per fer, com a mínim setmanalment, còpies de seguretat, tret que en el període esmentat no s'hagi produït cap actualització de les dades.*

2. Així mateix, s'han d'establir procediments per a la recuperació de les dades que garanteixin en tot moment la reconstrucció a l'estat en què estaven en el moment de produir-se la pèrdua o destrucció.

Únicament en cas que la pèrdua o destrucció afecti fitxers o tractaments parcialment automatitzats, i sempre que l'existència de documentació permeti assolir l'objectiu a què es refereix el paràgraf anterior, s'han de gravar manualment les dades de manera que quedi constància motivada d'aquest fet en el document de seguretat.

3. El responsable del fitxer s'ha d'encarregar de verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de seguretat i de recuperació de les dades.

4. Les proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent al tractament realitzat i s'anoti la seva realització en el document de seguretat.

Si està previst realitzar proves amb dades reals, prèviament s'ha d'haver realitzat una còpia de seguretat.

Article 102 RDLOPD.- *S'ha de conservar una còpia de seguretat de les dades i dels procediments de recuperació d'aquestes dades en un lloc diferent d'aquell en què estiguin els equips informàtics que els tracten, que ha de complir en tot cas les mesures de seguretat exigides en aquest títol, o utilitzant elements que garanteixin la integritat i recuperació de la informació, de forma que sigui possible la seva recuperació.*

Article 112 RDLOPD.- *1. La generació de còpies o la reproducció dels documents únicament pot ser realitzada sota el control del personal autoritzat en el document de seguretat.*

2. S'ha de procedir a la destrucció de les còpies o reproduccions rebutjades de manera que s'eviti l'accés a la informació que contenen o la seva recuperació posterior.

Situació actual:

A l'apartat 5.3.3 dels DS de Col·legiats, de Personal, i de Prevenció de Riscos Laborals, i a l'apartat 5.2.3 del DS d'Administració, s'estableix el procediment, periodicitat i custòdia per a la realització de les còpies de seguretat. Les disposicions contingudes es completen amb altres instruccions internes.

De la gestió del procediment de còpies de seguretat se n'encarreguen els tècnics informàtics de SOFTENG. A continuació detallarem els tipus de còpies de seguretat que es realitzen, però en tot cas cal aclarir prèviament que sempre són completes, en cinta DAT i realitzades a les 12h la nit.

Es fa una còpia diària de dilluns a divendres en el robot de cintes. Hi ha grups de cintes per dies, però aquestes diàries en cap cas surten del CPD.

La còpia realitzada el divendres serveix de còpia de seguretat setmanal. També es fa una còpia de seguretat mensual i anual. Aquests tres tipus de còpies són custodiades fora de la ubicació dels fitxers, fora del CPD per tant, i concretament dins de les instal·lacions d'una entitat bancària.

Els procediments establerts garantirien la reconstrucció de les dades d'un fitxer de fins a set dies abans aproximadament.

Hi ha un registre de backups que envia diàriament un e-mail als tècnics de SOFTENG indicant si la còpia de seguretat s'ha realitzat correctament o no. Si efectivament s'ha fet malament es revisa i es torna a executar durant el dia. A més a més, el procediment es verifica com a mínim un cop cada un o dos mesos.

Es fan proves prèvies a la implantació o modificació dels sistemes d'informació, però en tot cas sempre en un entorn de proves fictici, de preproducció.

Àrees de millora

No detectada.

De la verificació dels processos de recuperació i còpia de dades de caràcter personal s'hauria de deixar constància en un acta adjunta als Documents de seguretat. Recordem que en tot cas s'han de realitzar amb una periodicitat inferior als 6 mesos.

6.15. Registre d'accessos

Article 103 RDLOPD.- *1. De cada intent d'accés s'han de guardar, com a mínim, la identificació de l'usuari, la data i hora en què es va realitzar, el fitxer a què s'ha accedit, el tipus d'accés i si ha estat autoritzat o denegat.*

2. En cas que l'accés hagi estat autoritzat, és necessari guardar la informació que permeti identificar el registre a què s'ha accedit.

3. Els mecanismes que permeten el registre d'accessos han d'estar sota el control directe del responsable de seguretat competent sense que permetin la seva desactivació ni manipulació.

4. El període mínim de conservació de les dades registrades és de dos anys.

5. El responsable de seguretat s'ha d'encarregar de revisar almenys una vegada al mes la informació de control registrada i ha d'elaborar un informe de les revisions realitzades i els problemes detectats.

6. No és necessari el registre d'accessos definit en aquest article en cas que es donin les circumstàncies següents:

a) Que el responsable del fitxer o del tractament sigui una persona física.

b) Que el responsable del fitxer o del tractament garanteixi que únicament ell té accés a les dades personals i les tracta.

La concurrència de les dues circumstàncies a què es refereix l'apartat anterior s'ha de fer constar expressament en el document de seguretat.

Situació actual:

És necessari explicar en primer terme que només és preceptiva l'existència d'un registre d'accessos per a les bases de dades informàtiques que custodien dades de nivell alt, requisit que en el cas de l'entitat objecte d'auditoria no concorre.

No obstant, el programa de gestió col·legial manté un control específic de les accions que fa cada usuari a l'aplicació. Queda registrat el moment en què un usuari es connecta al sistema, i al moment en el qual es desconnecta. A més es pot monitoritzar posteriorment fent filtres per usuari o per dia. Registra tota la informació que l'usuari edita, insereix o elimina de la base de dades, creant així una taula de log de l'aplicació. A més, aquesta informació es pot consultar filtrant per usuari, entre dates, etc.

Tanmateix, la no necessitat de registre d'accessos suposaria també la no obligació d'elaborar informes de revisió mensual del sistema. Ara bé, per tal de permetre una certa traçabilitat del sistema de protecció de dades i encara en major motiu degut al recent trasllat d'ubicació física de l'entitat, s'elaboren amb una periodicitat mensual informes de revisió del sistema. En aquests informes, entre d'altres, es recullen els grans canvis generats pel trasllat esmentat però també incidències produïdes, quan ha resultat necessari sol·licitar diverses autoritzacions per al tractament d'imatges, etc.

Àrees de millora

No detectada.

Recomanem que l'entitat segueixi elaborant els esmentats informes de revisió mensual en els que hi faci constar les revisions realitzades i els problemes detectats, tant en fitxers automatitzats com no automatitzats.

6.16. Transmissió de dades a través de xarxes de comunicacions

Article 104 RDLOPD.- *Quan conforme a l'article 81.3 s'hagin d'implantar les mesures de seguretat de nivell alt, la transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fil de comunicacions electròniques s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers.*

Situació actual:

Es transmeten dades de caràcter personal a través de xarxes de telecomunicacions.

A continuació analitzarem els enviaments de dades més habituals però abans de tot cal esmentar que els correus electrònics que s'envien internament viatgen en tot cas per la xarxa interna, i per tant de forma xifrada.

En relació a temes de personal, la majoria de sortides de dades que s'efectuen són cap a organismes oficials com Hisenda o Seguretat Social i per portal web segur, però d'aquests tràmits s'encarrega FAURA-CASAS. Precisament les comunicacions amb aquesta empresa són per e-mail o per telèfon. L'entrega de les nòmines sempre es realitza directament a la persona interessada, de la mateixa manera que passa amb l'entrega de l'informe de la revisió mèdica.

Per una altra banda, les comunicacions amb els col·legiats i col·legiades solen produir-se o bé per e-mail, per telèfon, o en persona. També s'envia mensualment al *Consell de Col·legis de Catalunya* i a la *Organización Colegial de Enfermería* de l'Estat el llistat dels col·legiats al COIB. Aquest enviament es fa per correu electrònic.

Àrees de millora

No detectada.

6.17. Auditoria

Article 96 RDLOPD.- *1. A partir del nivell mitjà, els sistemes d'informació i instal·lacions de tractament i emmagatzematge de dades s'han de sotmetre, almenys cada dos anys, a una auditoria interna o externa que verifiqui el compliment del present títol.*

Amb caràcter extraordinari, s'ha de realitzar l'auditoria esmentada sempre que es facin modificacions substancials en el sistema d'informació que puguin repercutir en el compliment de les mesures de seguretat implantades, amb l'objecte de verificar-ne l'adaptació, adequació i eficàcia. Aquesta auditoria inicia el còmput de dos anys assenyalat en el paràgraf anterior.

2. L'informe d'auditoria ha de dictaminar sobre l'adequació de les mesures i controls a la Llei i el seu desplegament reglamentari, identificar les seves deficiències i proposar les mesures correctores o complementàries necessàries. També ha d'incloure les dades, fets i observacions en què es basin els dictàmens assolits i les recomanacions proposades.

3. Els informes d'auditoria els ha d'analitzar el responsable de seguretat competent, que n'ha d'elevar les conclusions al responsable del fitxer o tractament perquè adopti les mesures correctores adequades, i han de quedar a disposició de l'Agència Espanyola de Protecció de Dades o, si s'escau, de les autoritats de control de les comunitats autònomes.

Article 110 RDLOPD.- *Els fitxers inclosos en la present secció s'han de sotmetre, almenys cada dos anys, a una auditoria interna o externa que verifiqui el compliment del present títol.*

Situació actual:

L'entitat realitza enguany la seva tercera auditoria. La darrera data del mes de febrer de l'any 2008. Per tant, ha quedat acreditat l'entitat no ha seguit correctament el criteri de bienalitat establert reglamentàriament.

A més, i tot i que l'entitat manifesta que els informes van ser degudament tractats, no va quedar constància documental que les conclusions de l'auditoria realitzada l'any 2008 s'elevessin al responsable del fitxer.

Àrees de millora

Segons estableix la normativa aplicable, a partir del nivell mitjà els sistemes d'informació i instal·lacions de tractament i arxivament de dades s'han de sotmetre, almenys cada dos anys, a una auditoria, periodicitat que en aquest cas l'entitat no ha complert degudament.

Tanmateix i a diferència del que va succeir amb l'auditoria de l'any 2008, quan s'hagi rebut l'Informe d'Auditoria, el responsable de seguretat competent haurà d'elevar les conclusions al responsable del fitxer o tractament perquè adopti les mesures correctores adequades, i deixar-ne constància en una acta adjunta.

6.18. Criteris d'arxiu

Article 106 RDLOPD.- *L'arxivament dels suports o documents s'ha de fer d'acord amb els criteris que preveu la seva respectiva legislació. Aquests criteris han de garantir la correcta conservació dels documents, la localització i consulta de la informació i han de possibilitar l'exercici dels drets d'oposició al tractament, accés, rectificació i cancel·lació.*

En els casos en què no hi hagi cap norma aplicable, el responsable del fitxer ha d'establir els criteris i procediments d'actuació que s'hagin de seguir per a l'arxivament.

Article 108 RDLOPD.- *Mentre la documentació amb dades de caràcter personal no estigui arxivada en els dispositius d'emmagatzematge que estableix l'article anterior, pel fet d'estar en procés de revisió o tramitació, ja sigui prèviament o posteriorment al seu arxivament, la persona que se n'encarregui l'ha de custodiar i impedir en tot moment que hi pugui accedir una persona no autoritzada.*

Situació actual:

L'entitat disposa de diversos arxius en paper que custodien dades de caràcter personal, com a continuació analitzarem.

L'arxiu dels expedients dels treballadors es troba situat al despatx de Gerència, el qual sempre està tancat amb clau i quan hi ha d'accedir una persona diferent del Gerent hi ha d'estar degudament autoritzada. El considerat actiu, expedients dels treballadors que actualment estan prestant serveis a l'entitat, estan custodiats en un armari compacte ordenats per número correlatiu. En una caixa d'arxiu definitiu està el passiu dels expedients, dins del mateix despatx esmentat. Les nòmines estan en un arxivador anual, tot i que les més recents les custodia l'Auditor Intern al seu despatx.

Sens dubte que l'arxiu analitzar en més profunditat és el dels expedients dels col·legiats i col·legiades del COIB. Hi ha un arxiu dedicat a la planta baixa de les instal·lacions de l'entitat. En cap cas els expedients col·legiats surten d'aquest.

Per accedir-hi es necessita una clau que està custodiada pel personal de la recepció. Qui acostuma a entrar-hi més és el personal d'atenció al col·legiat. Cada cop que una persona pren la clau s'anota en un registre manual, concretament la persona corresponent i el motiu. El mateix succeeix quan es retorna. També hi ha un registre dins del propi arxiu dels moviments dels expedients, indicant també la persona i el motiu.

Els expedients es troben dins d'armaris de rodes, organitzats per número correlatiu i en etiquetes de colors, números que coincideixen amb els del programa ULISSES.

A data de la present auditoria no s'han destruït expedients, tot i que hi ha previst en un futur treure d'aquest arxiu els expedients de persones ja jubilades, èxitus i anteriors als 1932. Precisament aquests expedients van estar separats de l'arxiu durant un temps i custodiats per l'empresa LEINAD. Actualment estan en caixes.

També cal afegir que el transport dels expedients de l'antiga del Carrer Alcoi a l'actual va ser encarregat a l'empresa MOWIP. L'entitat manifesta que no es van produir incidències ni pèrdues d'informació durant aquestes tasques.

Fins a la data actual no s'han realitzats estudis que hagin requerit una revisió dels expedients col·legials, ni tampoc s'han detectat duplicitats.

També hi ha un arxiu general en el que es custodia documentació amb dades de caràcter personal, com la referent a comptabilitat, facturació, premis o cursos. Aquest arxiu està ubicat en una sala gran de la primera planta del COIB al que s'hi accedeix per clau que només en disposa el Responsable d'Arxiu i la persona de manteniment. Encara no es registren les entrades i sortides d'aquest arxiu, tot i que previst posar-ho en funcionament aviat.

La resta d'arxius que contenen dades de caràcter personal es limita al seu accés al personal degudament autoritzat i sempre en unes condicions òptimes de manteniment.

Àrees de millora

No detectada.

7. Conclusions (salvetats)

Inspeccionats tots els punts determinats pel Reglament de desenvolupament de la Llei orgànica 15/1999, de protecció de dades de caràcter personal, havent-se dut a terme les actuacions a les diferents dependències de l'entitat, realitzades les entrevistes amb els corresponents responsables d'àrea, havent-se valorat la documentació aportada, avaluats els sistemes de tractament de la informació, l'equip auditor detecta que les salvetats, de conformitat amb l'establert al RDLOPD, són:

- *Aspectes generals* (veure apartat 6.1)
- *Encarregat/s de tractament* (veure apartat 6.2)
- *Prestació de servei sense accés a dades personals* (veure apartat 6.3)
- *Règim de treball fora dels locals d'ubicació dels fitxers* (veure apartat 6.6)
- *Fitxers temporals* (veure apartat 6.7)
- *Document de Seguretat* (veure apartat 6.8)
- *Registre d'incidències* (veure apartat 6.10)
- *Gestió de suports i documents* (veure apartat 6.12)
- *Identificació i autenticació d'usuaris* (veure apartat 6.13)
- *Auditoria* (veure apartat 6.17)

Barcelona, Juny de 2010

Pere Ruiz Espinós

- Soci -