COL·LEGI OFICIAL D'INFERMERES I INFERMERS DE BARCELONA

INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Número de Protocol 7.466

ÍNDEX

1. Objectius i contingut

De conformitat amb el que estableix la normativa vigent sobre protecció de dades[1], tots els responsables de fitxer i/o encarregats de tractament 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.

[1] *Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (publicada en el BOE número 298, de 14 de desembre de 1999).*

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 (publicat en el BOE número 17, de 19 de gener de 2008).

2. 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.

Tant la planificació, com el treball de camp d'auditoria, com també l'elaboració d'aquest informe han estat desenvolupats per un equip de persones constituït per professionals qualificats en el camp de la protecció de dades de *Faura- Casas, Auditors- Consultors SL* 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, 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:

- ✓ Planificació dels treballs: identificació del/s centre/s de l'entitat i, en el seu cas, encarregat/s de tractament, objecte d'auditoria
- ✓ 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

3. Dades de l'entitat i treballs efectuats

3.1. Dades identificatives.

3.1.1. Dades entitat

Entitat	COL·LEGI OFICIAL D'INFERMERES I INFERMERS DE BARCELONA
NIF	Q- 0866003- G
Domicili	Carrer Pujades, 350 08019 Barcelona

3.1.2. Descripció de l'activitat

El **COL·LEGI OFICIAL D'INFERMERES I INFERMERS DE BARCELONA** (en endavant, l'Entitat), és una institució que vetlla per la defensa i representació corporativa de les infermeres i els infermers col·legiats a Barcelona, i que 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 de la 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.

3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en les diverses àrees i serveis de l'Entitat:

- Sistemes d'Informació i Informàtica
- Salut Laboral i Prevenció de Riscos Laborals
- Recursos Humans
- Arxiu
- Administració
- Facturació
- Comunicació
- Màrqueting
- Recerca/ Estudis
- Assessors externs (fiscal/tributari)
- Formació
- Col·legiació

Pel que fa als espais físics, s'han revisat els següents: planta baixa de l'edifici, on s'hi ubica l'assessor fiscal i tributari extern, l'Atenció al Col·legiat i l'Arxiu d'expedients de col·legiats; primera planta on s'hi ubica, entre d'altres, l'Arxiu General, Administració i Recursos Humans. Es visita, també, la sala CPD.

3.2.1. Data de realització de l'auditoria

Dies	4 i 5 de juny de 2012

3.2.2. Persones entrevistades i relació de la documentació lliurada a l'auditor

Persones entrevistades per ordre d'intervenció:

NÚMERO	PERSONA ENTREVISTADA	ÀREA DE TREBALL
1	Sr. Gabriel Bronchales	Responsable de Comptabilitat i de Qualitat
2	Sr. David Rangel	SOFTENG, SL, empresa encarregada dels Sistemes d'Informació de l'Entitat
3	Sra. Isabel Quintana	Prevenció de Riscos Laborals
4	Sra. Núria Garcia	Responsable de Recursos Humans
5	Sr. Jordi Cardila	Responsable d'Arxiu
6	Sra. Magda Tur	Àrea d'Administració
8	Sra. Gemma Bruna	Responsable de Comunicació
10	Sra. Laura Rausell	Administrativa que dóna suport a Recerca i a l'Àrea de Sistemes
11	Sr. Antoni de Alba	DENVER, Assessor fiscal
12	Sra. Sònia Navarro	Administrativa de l'Àrea de Formació
13	Sra. Rosa Rivas	Responsable de l'Àrea d'Administració Col·legial

Relació de la documentació lliurada a l'auditor:

Estatuts
Organigrama de l'Entitat i composició àrees Entitat
Sol·licituds de modificació de fitxers a l'Agència Espanyola de Protecció de Dades

Ultima versió dels Documents de Seguretat: Administració, Personal, Col·legiades i Prevenció de Riscos Laborals
Esquema de la xarxa informàtica
Descripció tècnica del nivell de seguretat dels productes de software destinats al tractament automatitzat de dades personals.
Instruccions de treball: Seguretat Informàtica i Pautes de Tractament d'Expedients col·legials
Procediment de gestió d'expedients
Contractes d'Encarregat de Tractament amb els diferents proveïdors
Mostreig de contractes d'encarregat de tractament amb els assessors externs Registre Entrada i Registre Sortida Sol·licitud alta nou usuari
Contracte cessió de dades Banc Sabadell
Registres d'accessos i registres d'entrades i sortides a l'arxiu general i a l'arxiu de col·legiats
Registres de seguiment setmanal, mensual i anual de les còpies de seguretat
Registre d'arxiu d'expedients
Models per a l'exercici dels drets ARCO
Formulari queixa
Sol·licitud de modificació permisos d'usuari
Document permisos carpetes compartides
Clàusula confidencialitat premis COIB
Clàusula LOPD inscripció Borsa de Treball
Model d'expedients de dades del col·legiat
Carta enviament anual cens col·legiats al *Consejo General*
Documentació Sol·licitud imatges Mossos d'Esquadra
Circular Informativa LOPD
Formulari de col·legiació

Resolució JUS/1099/2011, de 26 d'abril, per la qual es declara adequada a la legalitat la modificació de la denominació i del canvi de domicili dels estatuts del Col·legi Oficial d'Infermeres i Infermers de Barcelona, juntament amb una fotocòpia de la seva publicació en el DOGC núm. 5875, de 10 de maig de 2011

Recol·lecció de les dades:

- ✓ Relació dels fitxers, estructura i contingut
- ✓ Polítiques de seguretat i procediments (registre d'incidències, còpies de seguretat, identificació i autorització, esborrat de suports, xifrat, etc.)
- ✓ Document/s de Seguretat
- ✓ Auditories anteriors
- ✓ Disseny físic i lògic dels sistemes d'informació
- ✓ Relació d'usuaris, accessos autoritzats i funcions
- ✓ Inventari de suports i registre d'entrada i sortida de suports
- ✓ Registre d'accessos i informes de revisió dels mateixos
- ✓ Etc.

4. Anàlisi de les diferents àrees de l'auditoria

I - BLOC GENERAL

4.1. Auditoria.

Base legal: Articles 96 i 110 RD 1720/2007.

Situació actual

Els dies 4 i 5 de juny de 2012 l'Entitat realitzà la quarta auditoria en matèria de protecció de dades. L'auditoria anterior fou el juny del 2010, de manera que es realitza l'auditoria dins de la periodicitat biennal requerida per la normativa.

No obstant, l'Entitat afirma que, tot i haver realitzat unes conclusions de l'Informe d'Auditoria anterior, i elevar les mateixes al Responsable del Fitxer, per tal que adoptés les mesures correctores adequades, no en va deixar constància documental, incomplint d'aquesta manera l'article 96.3 Reial decret 1720/ 2007.

Àrees de millora

●	Àrea de millora	Les conclusions de l'auditoria han de ser analitzades pel Responsable de Seguretat, i les conclusions que extregui s'hauran d'elevar al Responsable del Fitxer, per tal que adopti les mesures correctores adequades, deixant-ne constància documental.

4.2. Aspectes generals.

Base legal: Articles 79, 80 i 81 RD 1720/2007.

Situació actual

D'ençà de l'anterior auditoria, l'Entitat ha canviat la seva denominació per "Col·legi Oficial d'Infermeres i Infermers de Barcelona", procedint a realitzar una modificació de la denominació dels fitxers davant l'AGPD , per als fitxers de naturalesa privada (Personal, Prevenció de Riscos Laborals i Administració), i del domicili.

Comentar que el fitxer de *col·legiats*, en tant que regula les dades dels col·legiats, revesteix naturalesa pública, ja que els col·legis professionals són considerats com a corporacions de dret públic (art. 35 L. 7/2006, de 31 de maig). En conseqüència, ha estat donat d'alta en el registre de l'APDCAT. No s'ha realitzat, però, la modificació de la denominació ni de l'adreça del fitxer de col·legiats davant l'APDCAT.

Els fitxers que té inscrits l'Entitat són els següents:

FITXER	CODI	FINALITAT	NIVELL	TRACTAMENT
ADMINISTRACIÓ	2042100220	Realització dels processos habituals de facturació, comptabilitat i financers de l'Entitat	Bàsic	Automatitzat
PERSONAL	2042100219	Gestió de Recursos Humans a efectes de selecció de personal, contractació, i elaboració i pagament de nòmines	bàsic	Automatitzat
COL·LEGIADES		Representació corporativa i assessorament en diversos camps a les col·legiades.	Mitjà	Automatitzat

Àrees de millora

●	Àrea de millora	L'Entitat cal que adapti el sistema de tractament dels fitxers declarats davant l'AGPD a la realitat existent, ja que si bé consta el tractament com a automatitzat la realitat mostra que es realitza un tractament de les dades de caràcter personal en suport mixt (tant en paper com informatitzades).

4.3. Document de seguretat.

Base legal: Articles 88, 95, 105 i 109 RD 1720/2007.

Situació actual

Mesures de seguretat
A. Existeix un document de seguretat per cada fitxer declarat o, per contra, es tracta d'un únic document de seguretat que inclou tots els fitxers declarats per l'entitat amb les especificitats pròpies de cadascun d'ells.
Comentaris: • L'Entitat ha elaborat un document de seguretat per a cadascun dels fitxers declarats davant l' AGPD, l'última versió dels documents de seguretat data de: ➢ Fitxer d'administració: 26/05/2010 ➢ Fitxer de personal: 26/07/2010 ➢ Fitxer de prevenció de riscos laborals: 26/05/2010 • Per al fitxer de col·legiats, inscrit davant l'APDCAT, també han elaborat el corresponent document de seguretat, l'última revisió del qual fou el 26/05/2010 • La normativa que es referencia en els documents de seguretat dels fitxers d'administració, personal, prevenció de riscos laborals i col·legiats és el Reial decret 994/1999, avui derogat pel Reial decret 1720/ 2007. • El fitxer d'administració estableix en el punt *1.4 nivell de seguretat del fitxer* que aquest és bàsic, mentre que en l'encapçalament del mateix es diu que és de nivell alt.

B. Àmbit d'aplicació del document amb especificació detallada dels recursos protegits:

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

Comentaris:

- No es fa referència a què existeixi un inventari actualitzat dels suports que tracten dades de caràcter personal.
- Caldria preveure en els documents de seguretat els accessos mitjançant targeta magnètica.
- Caldria adjuntar l'esquema de la xarxa existent.

C. Si s'escau, mesures alternatives quan no sigui possible establir sistemes d'obertura mitjançant clau o dispositiu equivalent a les portes dels armaris, arxivadors o altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal.

Si s'escau, mesures alternatives quan els armaris, arxivadors o altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal no es trobin amb àrees en què l'accés estigui protegit amb portes d'accés dotades de sistemes d'obertura mitjançant clau o un altre dispositiu equivalent *(nivell alt)*.

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

Comentari:

- Cal que l'Entitat protocol·litzi els criteris per al procediment relatiu a l'arxiu de documentació, així com establir per cada fitxer qui serà el responsable, i el període de conservació.
- Cal preveure l'existència d'un registre d'entrada i de sortida de documentació en els documents de seguretat del fitxer de personal, de prevenció de riscos laborals i de col·legiats. Pel cas que aquestes entrades/ sortides es vehiculin des de l'aplicatiu ULISSES caldrà preveure- ho també.
- En relació a tots els fitxers (excepte el d'administració, declarat de nivell bàsic), cal detallar l'existència d'un registre d'accessos a l'aplicatiu ULISSES.

- L'Entitat cal que revisi els punts *6* dels documents de seguretat per tal que contemplin la possibilitat d'exercir el dret d'oposició, així com també que es faci referència a la possibilitat d'exercir el dret de rectificació a través del formulari web.

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

F. Procediment de notificació, gestió i resposta davant les incidències.

G. Procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats.

H. 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.

Comentari:

- L'Entitat cal que faci constar en els documents de seguretat les mesures de seguretat preses en el trasllat de suports informatitzats, com és el cas de les còpies de seguretat.

- A banda, cal fer constar en tots els documents de seguretat el procediment de destrucció dels diferents suports (còpies de seguretat, ordinadors...) i documents (existència de trituradores, on estan ubicades...) amb dades de caràcter personal.

I. La identificació dels fitxers o tractaments que es tractin en concepte d'encarregat de tractament amb referència expressa al contracte o document que reguli les condicions de l'encàrrec, la identificació del responsable i del període de vigència de l'encàrrec, així com també si el tractament es realitza, o no, en els locals del responsable.

Comentari:

- L'Entitat cal que incorpori en els documents de seguretat un llistat actualitzat dels encarregats de tractament, i amb els camps que requereix la normativa.

J. Quan l'entitat actuï com a encarregat de tractament en els seus propis locals, aliens als del responsable del fitxer, ha de preveure en els documents de seguretat oportuns la identificació del fitxer o tractament i el seu responsable i les mesures de seguretat a implementar en relació amb el tractament.

Autoritzacions
K. Autorització per a l'emmagatzematge de dades de caràcter personal en dispositius portàtils (usuaris/perfils d'usuaris i període de validesa). Tractament de dades de caràcter personal en dispositius portàtils que no permetin el xifratge.
L. En relació al tractament de dades de caràcter personal fora dels locals del responsable, cal que hi hagi l'autorització així com també els usuaris/perfils d'usuaris i el període de validesa per a aquest tractament.
Comentari: • L'Entitat cal que incorpori una relació dels usuaris que tenen accés remot, així com el període de validesa d'aquests accessos. • Manca preveure en els documents de seguretat l'accés via web al correu electrònic que tenen alguns usuaris (indicar de quins usuaris es tracta i el període de validesa del mateix). • Pel que fa a l'ús d'USB, CD's, o altres dispositius (si bé aquests no són corporatius), recomanem a l'entitat que estableixi algunes instruccions sobre el seu ús, com per exemple en el *Manual d'Ús*, preveient les conseqüències per un mal ús, ja que, al estar els ports oberts, no es controla la informació que es pot extreure del centre.
M. Personal autoritzat per concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.
• Els documents de seguretat han de preveure el personal autoritzat per concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, que, segons hem descrit en el punt *4.11.* d'aquest Informe, correspon a l'administrativa de Sistemes d'Informació.
N. Personal autoritzat a accedir als llocs on estiguin instal·lats els equips físics que donin suport als sistemes d'informació. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.
Comentari • Cal establir en el punt *5.4* dels DS de personal i col·legiats i en el punt *5.5* de prevenció de riscos laborals, qui és el personal autoritzat a accedir a la sala de

servidors, així com preveure les mesures/autoritzacions a prendre pel responsable de seguretat, quan puntualment hi hagi d'accedir personal no autoritzat (neteja, manteniment, etc),

- En aquests punts dels DS es referencien diversos documents, els quals no ha quedat acreditat que existeixin. PR17-S01

O. Personal autoritzat a accedir als suports i documents que contenen dades de caràcter personal. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.

Comentari:

- Cal que en cada DS es faci constar o es redireccioni a la ubicació on es pot trobar el llistat d'usuaris autoritzats a accedir als diferents suports i documents que contenen dades de caràcter personal, segons de quin fitxer es tracti.

- A banda, s'hauria de preveure el procediment d'autorització per accedir als arxius i altres àrees amb dades de caràcter personal dels usuaris no autoritzats.

P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.

Comentaris:

- Qualsevol sortida de dades de caràcter personal fora de l'entitat ha de trobar- se degudament autoritzada, i s'ha de fer constar qui donarà aquestes autoritzacions.

Q. Personal autoritzat per a la recepció/ enviament de dades de caràcter personal *(nivell mitjà i/ o alt).*

Comentari:

- No es designa quins usuaris o perfils d'usuaris estan autoritzats a enviar/rebre dades de caràcter personal.

R. Personal autoritzat per a la realització del procediment de recuperació de dades.

Comentari • Manca preveure en els documents de seguretat qui és el personal autoritzat per a la realització del procediment de recuperació de dades. Manca preveure en els documents de seguretat qui és el personal autoritzat per a la realització del procediment de recuperació de dades.
S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.
Comentari: • Veure punt 4.4 de l'Informe.
Altres mesures
T. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat.
U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.
Comentari: • Manca preveure en els documents de seguretat la periodicitat del canvi de contrasenyes, tant al sistema com als aplicatius que accedeixen a dades de caràcter personal.
V. Pel cas que es realitzin proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal amb dades reals s'ha d'anotar la seva realització al document de seguretat.
W. Identificació del responsable de seguretat *(nivell mitjà i/ o alt).*
Comentari:

• Veure punt 4.4 Informe.
X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt)*.
Comentari: • Són exemples de controls periòdics les revisions que realitza l'Entitat de les còpies de seguretat.

Àrees de millora

●	Àrea de millora	Cal que els documents de seguretat estiguin sempre actualitzats a la realitat de l'entitat i a la normativa vigent. Cal que els documents de seguretat es completin en els termes esmentats en el quadre anterior, que són les exigències mínimes reglamentàries. La major part dels aspectes pendents de desenvolupar poden estar en el propi DS, o bé en els seus annexos.

4.4. Delegació d'autoritzacions.

Base legal: Article 84 RD 1720/2007.

Situació actual

En el *punt 5.2* dels DS de personal, prevenció de riscos laborals i col·legiats es fa referència a que el responsable de seguretat serà l'encarregat de coordinar i gestionar les mesures de seguretat definides pel responsable del fitxer.

Tot i així, no es preveuen les delegacions que el Responsable del Fitxer realitza a altres persones, com per exemple:

- El personal autoritzat a concedir, alterar o anul·lar l'accés autoritzat.
- Revisió de les còpies de seguretat.

Àrees de millora

●	Àrea de millora	A dia d'avui el Responsable del Fitxer delega diferents funcions que li corresponen, si bé aquestes delegacions no es troben documentades.

4.5. Tercers.

ENCARREGATS DE TRACTAMENT

Base legal: Article 82 RD 1720/2007.

Situació actual

Un cop realitzat el mostreig de les relacions d'encarregats de tractament, passem a comentar el següent:

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
FAURA-CASAS, AUDITORS I CONSULTORS, SL	Assessorament fiscal i laboral.	☑	Disposen de contracte d'acord amb les previsions de l'article 12 LOPD.
ASSESSORS EXTERNS	Assessorament jurídic al col·legiat en diversos camps.	☑	El contracte de prestació de serveis incorpora a la clàusula 5ena i 6ena el tractament de dades de caràcter personal, si bé no s'especifica quines mesures de seguretat concretes adopta l'encarregat de tractament en relació amb les dades de caràcter personal titularitat de l'Entitat, tal i com exigeix l'article 12 LOPD.
SOFTENG, S.L.	Manteniment i suport informàtic.	☑	Disposen de contracte d'acord amb les previsions de l'article 12 LOPD.
STAFF CONSULTANTS	Gestió de *software* de la borsa de treball.	☑	El contracte d'encarregat de tractament no preveu les mesures de seguretat concretes que adopta l'encarregat de tractament en relació a les dades de caràcter personal titularitat de l'Entitat, tal i com exigeix l'article 12 LOPD.

			D'altra part, en el contracte no s'hi preveuen tots els serveis que presta l'encarregat de tractament, ja que s'ha constatat que també realitza la gestió del *software* de la borsa de treball.
GESIO SOLUTIONS, SL	Enviament per correu electrònic als col·legiats COIBDigital.	☑	Disposen de contracte d'acord amb les previsions de l'article 12 LOPD.
DELEGATS COMARCALS	Representació i assessorament dels col·legiats a diverses delegacions comarcals del territori de Barcelona.	☑	La clàusula 6ena del contracte no preveu les mesures de seguretat concretes que adopta l'encarregat de tractament en relació amb les dades de caràcter personal titularitat de l'Entitat, tal i com exigeix l'article 12 LOPD.
SERVICIOS PLENOS DE MANIPULACIÓN, SL	Serveis de manipulació, impressió i ensobrat de correu ordinari.	☑	Disposen de contracte d'acord amb les previsions de l'article 12 LOPD.
SECURITAS	Vigilància i seguretat	☑	El contracte d'encarregat de tractament no preveu les mesures de seguretat que adopta l'encarregat en relació a les dades de caràcter personal titularitat de l'Entitat.

A banda dels encarregats de tractament detectats, s'ha constatat l'existència d'un contracte de cessió de dades amb BANC SABADELL, SA, amb motiu de la "Campanya del Compte Expansió PRO", dirigida als col·legiats, on se cedeixen les dades dels interessats que hagin prèviament prestat el seu consentiment. El contracte, de data 14 de maig de 2012, preveu totes les clàusules relatives a la normativa en matèria de protecció de dades.

Àrees de millora

●	Àrea de millora	Veure comentaris del quadre anterior. *Veure punt 4.3.1 de l'Informe d'Auditoria.*

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

No ha quedat acreditada l'existència de tercers sense accés a dades de caràcter personal, tals com personal de neteja extern o serveis diversos de manteniment (ex: elèctric, pintors, etc.)

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS	COMENTARIS
INTEGRAL FACILITY SEVEN, SL	Serveis de neteja.	☑	El contracte inclou la clàusula 7ena sobre confidencialitat, en els termes previstos en l'article 83 del Reial decret 1720/ 2007.
SERKONTEN, SAU	Serveis de controls de plagues.	☑	El contracte inclou la clàusula 7ena sobre confidencialitat, en els termes previstos en l'article 83 del Reial decret 1720/ 2007.

Àrees de millora

▲	No detectada	

4.6. Legitimació de dades.

Base legal: Articles 5 i 6 LOPD 15/1999.

Situació actual

L'Entitat inclou en el punt *5.1.2* de cada document de seguretat una previsió a la legitimació en la recollida de dades, especificant en el DS d'administració que no serà necessari ja que les dades provenen de factures i altres documents assimilats.

S'analitza a continuació on s'evidencia la legitimació de les dades de cada fitxer de l'entitat:

FITXER	LEGITIMACIÓ	COMENTARIS
Personal	Quan un treballador s'incorpora a l'Entitat se li fa entrega del full d'informació sobre el tractament de les seves dades de caràcter personal, d'acord amb l'article 5 LOPD.	Aquest document compleix amb els requisits exigits per la normativa vigent. Tanmateix, pel cas que l'Entitat opti per modificar el sistema de tractament dels fitxers, en els termes ja indicats en el punt 4.2 d'aquest Informe, caldrà realitzar les oportunes modificacions a aquest document.
	En relació a l'autorització per a la presa d'imatges en cada cas concret en què es procedeix a gravar imatges o a fer fotografies de treballadors se'ls demana la corresponent autorització.	Aquest document compleix amb els requisits exigits per la normativa vigent.
	L'Entitat rep currículums *vitae* (CV) de persones interessades a prestar- hi els seus serveis, que s'entreguen en mà o per	Aquest document compleix amb els requisits exigits per la normativa vigent.

	correu electrònic. També fan convocatòries en les borses de treball de les universitats. A tots els CV que es reben se'ls dóna resposta d'acord amb l'article 5 LOPD.	
Col·legiats/ Col·legiades	L'alta com a col·legiat del COIB pot ser una alta nova o per trasllat. En ambdós casos es fa entrega als nous col·legiats del full d'informació sobre el tractament de les seves dades de caràcter personal. Aquest document també preveu la possibilitat de què el col·legiat doni el seu consentiment per tal que les seves dades de caràcter personal puguin ser cedides a altres entitats per tal que ofereixin als col·legiats serveis de valor afegit.	Aquest document compleix amb l'article 5 i 6 LOPD.
	Els col·legiats del COIB poden sol·licitar el trasllat del seu expedient a un altre Col·legi, en persona o mitjançant la pàgina de l'Entitat. Segons manifesta l'Entitat, el formulari per aquests casos inclou una clàusula d'informació sobre el tractament de les dades de caràcter personal d'acord amb els requisits de l'article 5 LOPD.	

	El formulari web de contacte amb el COIB inclou una clàusula informativa sobre el tractament de les dades de caràcter personal introduïdes, d'acord amb l'article 5 LOPD.	
	Segons manifesta l'Entitat, el formulari web de modificació de dades dels col·legiats inclou una clàusula informativa sobre el tractament de les dades de caràcter personal, tal i com exigeix l'article 5 LOPD.	
	Segons manifesta l'Entitat, s'inclou la clàusula informativa sobre el tractament de dades de caràcter personal en el formulari de baixa del COIB.	
	Quan un col·legiat agafa un llibre de la Biblioteca en préstec se li demanen un seguit de dades de caràcter personal, si bé no s'informa sobre el tractament de les mateixes tal i com exigeix l'article 5 LOPD. L'Entitat ja ha començat a treballar per tal de subsanar aquest aspecte.	En qualsevol procés de recollida de dades de caràcter personal l'Entitat cal que compleixi amb l'article 5 LOPD.
	Els col·legiats poden sol·licitar informació sobre alguns dels serveis i descomptes especials (serveis de valor afegit) que ofereix el COIB en col·laboració amb diverses entitats (DIR, Banc Sabadell, etc.) Al sol·licitar aquesta informació telefònicament, se li enviarà un *e-mail* a l'interessat, especificant que si vol que se li doni aquesta informació haurà de contestar autoritzant expressament la cessió de les seves dades a les entitats per les quals sol·licita informació.	Aquest document compleix amb els requisits exigits per la normativa vigent.

	Es compleix així amb les exigències dels articles 5 i 6 LOPD.	
	L'Entitat posa a l'abast de qualsevol usuari els fulls de queixa.	En aquest formulari no es preveu la clàusula conforme els articles 5 LOPD.
	Quan l'Entitat realitza el certamen anual de la convocatòria dels premis COIB n'informa els col·legiats en els termes de l'article 5 LOPD.	Aquest document compleix amb els requisits exigits per la normativa vigent.
	L'Entitat realitza periòdicament sessions de formació per a col·legiats, segons manifesta l'Entitat en la inscripció a aquestes formacions s'informa al col·legiat sobre el tractament de les seves dades de caràcter personal en els termes de l'article 5 LOPD.	Aquest document compleix amb els requisits exigits per la normativa vigent.
	L'entitat envia diferents *newsletters* periòdicament tant a col·legiats com a treballadors: - El COIB flaix, per temes de calendari, enviat per correu ordinari - El Butlletí Influeixes@, cada 15 dies, per correu electrònic - La revista trimestral Influeixes - *Mailings* per correu ordinari, amb publicitat, de manera molt puntual	Per a tots aquests tractaments de dades s'ha donat als diferents destinataris la informació requerida i s'ha recavat el consentiment en els termes de la LOPD, de tal forma que només reben les diferents *newsletters* si han atorgat prèviament el seu consentiment.
	Quan el col·legiat ha realitzat un curs de formació, se li pot emetre una factura si aquest ho demana, on s'inclouen totes les dades del curs que ha realitzat, així com les seves pròpies	Es recomana que s'inclogui la clàusula esmentada sobre el dret d'informació previst a l'article 5 LOPD en les factures realitzades a persones físiques.

	identificatives.	

Àrees de millora

●	Àrea de millora	*Veure comentaris del quadre anterior.*

4.7. Drets ARCO.

Base legal: Articles 15-17 LOPD 15/1999.

Situació actual

Els punts *6* dels documents de seguretat *Exercici i tutela dels drets dels afectats* estableixen que els usuaris podran exercir, en relació a les dades contingudes en cada fitxer, el dret d'accés, rectificació i cancel·lació de les seves dades mitjançant sol·licitud al responsable del fitxer de l'Entitat. S'adjunten com annex els formularis per a l'exercici dels tals drets.

No es fa referència ni es disposa, però, del corresponent formulari per a l'exercici del dret d'oposició. A banda, els models actuals incorporen com a normativa de referència el Reial decret 1332/ 1994, derogat pel Reial decret 1720/ 2007.

L'Entitat manifesta que tan sols s'exerceixen els drets de rectificació, per actualitzacions de dades d'algun col·legiat (canvi d'adreça, telèfon, etc.) i que molts cops els usuaris els exerceixen telefònicament, com per exemple quan s'apunten a un curs de formació, quan s'aprofita per comprovar que les dades de l'usuari estan actualitzades. Aleshores es procedeix a modificar les mateixes segons les instruccions de l'usuari.

D'altra part, tal i com comentàvem al punt anterior, l'Entitat disposa a la web d'un formulari de modificació de dades.

Àrees de millora

●	Àrea de millora	L'Entitat cal que revisi els models per a l'exercici dels drets ARCO per tal d'adaptar- los a la normativa vigent (el Reial decret 1720/ 2007). L'Entitat cal que procedeixi a tractar la modificació/ rectificació de dades com un dret ARCO, dins de la mesura del possible. *Veure punt 4.3.D de l'Informe.*

II - BLOC DE MESURES INFORMÀTIQUES

4.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'Entitat ha elaborat un esquema de la xarxa, que si bé no s'incorpora com annex als documents de seguretat, sí que podem dir que en els punts 2 dels documents de seguretat es fa una breu referència a la xarxa existent, especialment en temes de software. D'altra part, l'Entitat també disposa del document *Instrucció de Treball- Seguretat Informàtica*.

L'accés dels usuaris a les dades es produeix a través d'una xarxa interna LAN cablejada, enllaçada a tots els equips informàtics a través de fibra òptica.

La seguretat de la xarxa queda garantida mitjançant.

- *Firewall* restrictiu de ports i de control d'atacs externs, realitzada pel servidor ISA
- Antivirus Kaspersky per als protocols http, ftp i smtp.
- Antivirus d'actualització diària per als fitxers del propi servidor o qualsevol dispositiu dels clients-usuaris.
- Filtres anti-spam, que analitzen tot el tràfic del correu electrònic.

Per garantir la seguretat de la xarxa es revisa de forma automatitzada l'estat dels servidors. A més a més, es revisa permanentment l'estat de la temperatura, càrrega del CPU, consum de memòria, etc.

Pel que fa a l'accés a través de WI-FI es disposa d'una xarxa, aïllada físicament dels servidors interns, per als cursos de formació o, en general, per a qualsevol usuari extern que dins les dependències de l'Entitat requereixi de connexió a Internet.

Tots els treballadors de l'entitat disposen de correu electrònic (@coib.cat), que s'atorga a l'incorporar- se a l'Entitat, que disposa d'un certificat SSL per encriptar la connexió.

Pel que fa als col·legiats, també se'ls atorga un correu electrònic (@coib.net), les dades dels quals es troben en un altre servidor Data Center. No obstant, l'Entitat manifesta que l'ús real del mateix pels col·legiats és molt escàs.Les aplicacions detectades durant el treball de camp utilitzades per l'Entitat i en les quals es tracten dades de caràcter personal es detallen a continuació:

APLICACIÓ	UTILITAT
ULISSES	Gestió col·legial.
CONTAPLUS	Comptabilitat (comentar que en aquest aplicatiu en principi no hi hauria d'haver

	dades de caràcter personal).
A3-Nom	Gestió de recursos humans.
IMMAGIC	Gestió de l'Arxiu i la Biblioteca (comentar que en aquest aplicatiu en principi no hi hauria d'haver dades de caràcter personal).
LINK	Control horari del personal a partir de l'activitat dels equips i que s'integra amb l'OUTLOOK.
XXXXX	Software per a la configuració de les targes d'accés físic.
MICROSOFT OFFICE	Processador de textos i altres utilitats.

Comentar que per a la realització de la transferència de nòmines l'Entitat es connecta al Banc de Sabadell On- line.

Àrees de millora

▲	No detectada	

4.9. Connexions remotes.

Base legal: Article 86 RD 1720/2007.

Situació actual

Es produeixen tractaments de dades de caràcter personal fora dels locals on es troben ubicats els fitxers.

D'una banda, s'observa que l'accés remot es produeix via Terminal Server i existeix un servidor específic per aquest tipus d'accés.

Els usuaris que disposen d'accés remot per connectar-se han d'introduir el mateix nom d'usuari que tenen per accedir al sistema i una *password*.

Els usuaris que tenen correu electrònic també poden connectar- se a aquest via web (OWA).

Àrees de millora

▲	No detectada	*Veure punt 4.3.L de l'Informe*

4.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

En primer terme, i tal i com ja hem tractat en el punt 4.8 d'aquest Informe, cal posar de manifest que tots els treballadors de l'Entitat, així com els col·legiats, disposen de correu electrònic personal (@coib.cat i @coib.net respectivament).

L'accés al correu electrònic a través de l'Outlook tan sols es pot fer dins la xarxa.

Pel que fa a la transmissió de dades de personals mitjançant xarxes de telecomunicacions (e-mail, fax...), s'han detectat en les següents àrees:

- Prevenció de riscos laborals → S'envia un correu electrònic amb el nom i el DNI en el cas d'accidents de treball, però no s'hi associen dades de salut.

- Recursos Humans →S'envien correus electrònics a la gestoria que tramita les altes i baixes dels treballadors. També es reben les nòmines i el resum mensual per correu electrònic.
- Arxiu d'expedients → Quan un col·legiat demana el trasllat d'expedient a un altra Col·legi, s'envia un fax al nou centre, on s'indica tan sols el nom i cognom del col·legiat.

- Facturació → S'envia un Excel per correu electrònic a la gestoria fiscal, amb el llistat dels treballadors a qui s'ha fet la corresponent reducció d'IRPF.

Àrees de millora

▲	No detectada	

4.11. Control d'accés.

Base legal: Articles 89.1 i 91 RD 1720/2007.

Situació actual

L'Entitat disposa del document *Grup Carpetes Compartides* que conté al llistat de cadascun dels usuaris que poden accedir a les mateixes. D'altra part, els documents de seguretat contemplen algunes referències en el punt *5.3.1* (DS del fitxer de personal, del de col·legiats i del de prevenció de riscos laborals) i en el punt *5.2.1* en el cas del DS del fitxer d'administració.

Les funcions i obligacions dels perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació es troben clarament definides. Per tant, els usuaris només poden accedir a les dades i als recursos que necessiten per al desenvolupament de les seves funcions. Els mecanismes que impedeixen que els usuaris accedeixin a més dades de les autoritzades és l'ús de contrasenyes.

L'Entitat manifesta que, dins d'un mateix departament/ àrea, pot haver-hi diferents perfils d'usuari, ja que cadascú pot tenir accés, per raó de les seves funcions, tan sols a determinades carpetes.

Pel que fa al sistema d'alta d'usuaris, quan un treballador s'incorpora a l'Entitat, la persona encarregada (administrativa de l'Àrea de Sistemes) li assigna els permisos que li pertoquen en funció del rol que ocuparà dins l'Entitat.

Pel que fa a les modificacions i baixes l'Entitat disposa del corresponent formulari per tal de què la persona encarregada pugui procedir a l'efecte.

Pel que fa als usuaris remots, se'n donarà habilitació quan existeixi una autorització expressa per part de Gerència.

Àrees de millora

▲	No detectada	*Veure punt 4.3.M de l'Informe.*

4.12. Identificació i autenticació d'usuaris.

Base legal: Articles 93 i 98 RD 1720/2007.

Situació actual

Tots els usuaris amb accés al sistema, al correu electrònic i a les aplicacions disposen d'usuari i contrasenya individualitzat, de manera que es garanteix la correcta identificació i autenticació dels usuaris.

La identificació de qualsevol usuari per accedir al sistema, al correu electrònic i a les aplicacions és inequívoca i personalitzada, mitjançant la primera lletra del nom i el primer cognom sencer.

Quan es realitza una alta d'un usuari se li dóna una contrasenya, que haurà de modificar obligatòriament el primer cop que es connecti.

Les contrasenyes, que hauran de tenir 8 dígits alfanumèrics, s'emmagatzemen al sistema de forma inintel·ligible, de manera que, si a un usuari se li bloqueja el sistema per reiterats accessos erronis, aquesta no es podrà recuperar de cap manera, sinó que se li haurà d'atorgar una contrasenya nova.

S'ha constatat que a dia d'avui molts aplicatius no contemplen la caducitat de les seves contrasenyes (excepte el CONTA PLUS, tot i que no conté dades de caràcter personal), tot i que l'Entitat manifesta que està en procés de canvi imminent.

El bloqueig de pantalla davant de la inactivitat es troba activat en tots els ordinadors, i salta al detectar-se entre 2 i 5 minuts d'inactivitat.

Àrees de millora

●	Àrea de millora	Cal que l'Entitat estableixi una periodicitat en el canvi de contrasenyes dels aplicatius que no ho contemplin, com a mínim un cop l'any. Tal fet s'haurà de fer constar degudament en els documents de seguretat.

4.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

L'Entitat no és titular de dades de caràcter personal, no resultant d'aplicació les consideracions relatives al registre d'accessos.

Àrees de millora

▲	No detectada	

4.14. Còpies de seguretat.

Base legal: Articles 94, 102 i 112 RD 1720/2007

Situació actual

Els punts *5.2.3.* del DS d'administració, el *5.3.3.* del de col·legiats, personal i prevenció de riscos laborals preveuen a grans traços el procediment, periodicitat i custòdia de les còpies de seguretat, que es complementen amb la *Instrucció de Treball – Seguretat Informàtica*.

Pel que fa a les còpies setmanals, mensuals i anuals, es guarden en una caixa forta ignífuga, ubicada a la mateixa sala de servidors.

Amb una periodicitat quinzenal o mensual s'extreuen les còpies setmanals i mensuals de l'Entitat, portant-les al Banc de Sabadell, on es custodien. Quan es porten les còpies, el Banc Sabadell atorga a l'Entitat un document, conforme es deixen allà.

L'Entitat manifesta que, aproximadament, amb una periodicitat mensual es realitzen les corresponents proves de recuperació de dades en cadascuna de les àrees de l'Entitat, garantint d'aquesta forma allò previst en l'article 94.3 del Reial decret 1720/ 2007: s'intenten recuperar els fitxers de les carpetes compartides i de les carpetes pròpies d'algun usuari de la còpia mensual abans d'enviar la cinta corresponent al Banc de Sabadell. Cada mes es va rotant per diferents àrees. Tanmateix, no es deixa constància d'aquestes revisions.

D'altra part, en cas que surti alguna còpia errònia o que no es realitzi correctament, s'envia un correu electrònic a Sistemes d'Informació, juntament amb la prova mensual de recuperació del document, tot i que l'Entitat afirma que amb el sistema actual de realització de les còpies (Snap Shots), no és possible que hi hagi errors.

No es té constància que l'Entitat realitzi proves amb dades reals.

Àrees de millora

▲	No detectada	

4.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

És inherent al funcionament de qualsevol entitat la generació de fitxers ofimàtics temporals, i més si es té en compte que es disposa de MICROSOFT OFFICE. De moment l'Entitat manifesta que cada usuari té espai a les seves carpetes personals, i que no han establert quotes d'usuari perquè encara tenen espai de sobres al servidor.

No obstant, l'Entitat manifesta que periòdicament recorda als treballadors la necessitat d'eliminar els fitxers temporals, tot i que finalment acaba sent responsabilitat de cada usuari eliminar- los. Del mateix mode, si es detecten documents duplicats, es recomana a l'usuari que n'esborri un.

A la carpeta compartida per tots els usuaris, un cop al mes es realitza una alineació de fitxers, ordenats per data de creació, i tots aquells amb una antiguitat superior als 30 dies són eliminats.

Àrees de millora

▲	No detectada	Recomanem a l'Entitat que plasmi les conductes existents en relació als fitxers temporals al document *Normes d'Ús*. .

4.16. Registre d'entrades i sortides de suports automatitzats.

Base legal: Article 97 RD 1720/ 2007.

Situació actual

Comentar que a nivell de document de seguretat es preveu en el punt *5.8.1*. del fitxer de prevenció de riscos laborals i en el punt *5.7.1* del fitxer de col·legiats l'existència d'un registre d'entrada i sortida de suports informàtics a l'exterior, la utilització del qual ha quedat acreditada.

En relació als suports informàtics comentar que la sortida de còpies de seguretat queda registrada.

Àrees de millora

▲	No detectada	

III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS

4.17. Dispositius portàtils, inventari, etiquetatge, xifrat i destrucció de suports i documents.

Base legal: Articles 86, 92, 101 i 112 RD 1720/ 2007.

Situació actual

En el si de l'entitat pràcticament no s'utilitzen dispositius portàtils: no fan ús d'ordinadors portàtils fora del centre, i cap PC disposa del *software* necessari per tal de poder gravar CD'S, ni es disposa d'USB's corporatius.

De totes maneres, els ports USB dels ordinadors de l'entitat Estan habilitats, permetent així que es pugui extreure informació.

No ha quedat acreditat que els dispositius per a la realització de les còpies de seguretat es trobin encriptats o disposin de contrasenya.

L'entitat manté un inventari i etiquetatge dels suports informàtics que contenen dades de caràcter personal, el qual es troba permanentment actualitzat. L'última revisió es realitzà el passat mes de maig de 2012.

No existeix cap protocol de destrucció de suports que continguin dades de caràcter personal ja que fins al moment l'Entitat encara no ha destruït res. Tanmateix, quan es va produir el canvi de domicili social, alguns equips es van enviar el Camerun, prèvia neteja total de tot el disc dur.

L'entitat comenta que qualsevol tipus de reparació de suports es duu a terme a les pròpies instal·lacions.

Àrees de millora

▲	No detectada	

4.18. Control d'accés.

Base legal: Articles 107, 108 i 111 RD 1720/ 2007.

Situació actual

Pel que fa als dispositius d'emmagatzematge, i als sistemes que dificulten l'obertura d'aquests, i el tancament dels espais on es troben aquests dispositius es contemplen algunes referències en el punt *5.4* dels DS dels fitxers de personal i de col·legiats, i el *5.5* del fitxer de prevenció de riscos laborals

Tots els despatxos disposen de tancament amb clau, i aquells en els que es guarda documentació hi ha armaris que estan tancats amb clau.

Pel que fa a l'Arxiu General, ubicat a la primera planta de l'edifici, s'hi troba la documentació relativa a comptabilitat, correspondència, Gerència, cursos de formació i fotografies. En definitiva la documentació interna de tot el Col·legi.

L'Entitat manifesta que l'arxiu d'expedients dels treballadors (excepte les nòmines pendents de repartir) i el de facturació es troben a l'Àrea de Gerència, i que aquest roman en un armari tancat amb una clau. A banda, es disposa d'un arxiu passiu de personal.

Pel que fa a les nòmines pendents de repartir, aquestes s'ubiquen a un armari d'Administració, al que només s'hi pot accedir a través de clau.

L'Arxiu Prevenció de Riscos Laborals conté dades d'accidents laborals, juntament amb alguna dada de salut i baixes professionals. L'accés és a través de clau. El CPD del servidor esta ubicat en una sala tancada amb clau.

Àrees de millora

▲	No detectada	*Veure punt 4.3.D. de l'Informe.*

4.19. Registre d'accessos.

Base legal: Article 99 i 113 RD 1720/2007.

Situació actual

L'Entitat disposa de mecanismes que permeten identificar, en la majoria de casos, els accessos realitzats en el cas de documents que puguin ser utilitzats per múltiples usuaris.

Per tal d'aconseguir la identificació d'aquests accessos l'Entitat disposa d'una política de claus, així com targetes d'accés personal, i diversos llistats d'accés als arxius de documentació que hi puguin accedir múltiples usuaris:

- Pel que fa a l'Arxiu general, així com els de Recursos Humans, Administració i Facturació, únicament els seus responsables tenen la clau d'accés, de tal forma que qualsevol altre usuari que hi vulgui accedir haurà de fer-ho prèvia sol·licitud expressa al seu responsable.

- Existeix un registre d'accessos a l'arxiu de la planta baixa de l'edifici al que només pot accedir- hi personal autoritzat, previ registre.

- Pel que fa a la resta de personal, cada treballador, assessor extern i personal de Junta disposa d'una targeta per accedir a les àrees corresponents, segons el perfil d'usuari assignat d'acord amb les funcions que desenvolupa a l'Entitat.

Àrees de millora

▲	No detectada	

4.20. Criteris d'arxiu.

Base legal: Articles 106 RD 1720/2007.

Situació actual

L'Entitat manifesta que els criteris d'arxiu s'estableixen per temes, dividint-se bàsicament en llocs de treball, formació i vigilància de la salut. Dins de cada carpeta, s'ordenen per anys (2010, 2011, 2012...), i es divideixen entre l'arxiu actiu (de l'actualitat, fins a 5 anys enrere), i passiu (més de 5 anys d'antiguitat).

Pel que fa a l'arxiu general, l'Entitat manifesta que en l'últim any ha estat reorganitzant i reordenant el mateix, tot i que encara no han destruït documentació. Cada document que s'hi custodia es troba enregistrat i detallat.

Durant els treballs de camp es va constatar que l'Entitat no protocol·litzat t cap política o protocols de criteris d'arxiu, tot i que de moment tampoc han destruït cap documentació en cap dels departaments del Col·legi, només en el cas que es tracti de duplicats. Manifesten, però que tenen la intenció de començar a fer-ho.

Àrees de millora

▲	No detectada	*Veure punt 4.3.D de l'Informe*

4.21. Entrades i sortides de documents.

Base legal: Articles 97 i 114 RD 1720/2007.

Situació actual

El document de seguretat del fitxer de prevenció de riscos laborals (punt *5.8.1*) i el de col·legiats (punt *5.7.1*) únicament es refereixen a l'existència d'un registre d'entrada i sortida de suports informàtics a l'exterior, sense fer esment als suports físics o documents.

El document de seguretat del fitxer de personal, per la seva banda, no preveu en cap punt cap tipus de registre d'entrada i sortida

Per últim, el document de seguretat del fitxer d'administració tampoc ho preveu, però al ser un fitxer amb dades de caràcter personal de nivell bàsic, no és necessari segons el RD 1720/2007.

Tot i l'anterior, durant els treballs de camp es detectà que l'Entitat disposa de diversos registres d'entrada i sortida de documentació dins de la mateixa Entitat que conté dades de caràcter personal de nivell mitjà i/o alt: concretament, un per a l'arxiu general i un per a l'arxiu de la planta baixa.

Tanmateix, durant els treballs de camp es detectaren moviments d'entrada i sortida a/de l'exterior de l'Entitat, que no quedaven registrats directament, com per exemple quan es demana el trasllat d'un expedient de col·legiat a un altre Col·legi, que s'envia per correu postal. la traçabilitat d'aquests moviments es pot aconseguir a través de l'ULISSES.

Àrees de millora

●	Àrea de millora	L'Entitat cal que registri totes les entrades i sortides de documentació amb dades, especialment les que surten a l'exterior de les instal·lacions. Pel cas que aquest aspecte es vehiculi a través de l'ULISSES caldrà plasmar- ho en el document de seguretat oportú. El registre haurà de permetre conèixer, directament o indirectament, els camps que s'especifiquen a continuació: *tipus de document_ data i hora d'enviament/ recepció_ emissor_ nombre de documents enviats/rebuts_ tipus d'informació que contenen_ forma d'enviament/ lliurament_ persona responsable de la recepció/lliurament, que haurà d'estar degudament autoritzada.* *Veure punt 4.3.D de l'Informe*

4.22. Fitxers temporals.

Base legal: Articles 87 i 112 RD 1720/2007.

Situació actual

En el si de l'Entitat es generen alguns fitxers temporals en suport paper. A les instal·lacions de l'Entitat s'hi ubiquen diferents destructores de paper (una a cada Àrea), que garanteixen que, un cop desapareguda la necessitat que va motivar la creació del document, aquest sigui destruït.

El personal sap que per als documents que continguin qualsevol tipus de dada personal o confidencial hauran de ser destruïts en les corresponents destructores, i mai llençar-los a la paperera, impedint- ne així la seva posterior recuperació.

Tanmateix, ni en el *Manual de Normativa Laboral* ni en les *Normes d'Ús* es preveu cap clàusula sobre la obligació de destruir el paper confidencial en les destructores corresponents.

Àrees de millora

▲	No detectada	D'igual manera, es recomana a l'Entitat que incorpori en la *Normativa Laboral* o en les *Normes d'Ús* alguna previsió relativa a la destrucció de documentació confidencial, establint la prohibició de llençar la mateixa a les papereres de brossa.

III- BLOC DE MESURES ORGANITZATIVES

4.23. Registre d'incidències.

Base legal: Articles 90 i 100 RD 1720/2007.

Situació actual

En el punt *5.7.2* del DS del fitxer de col·legiats, *5.6.1*. del de personal i *5.8.3* de prevenció de riscos laborals es preveu l'existència d'un registre d'incidències que afecten a la seguretat de les dades, i se'n regula la descripció, malgrat que no es descriu amb precisió el procediment a seguir en detectar una incidència, o com es pot resoldre aquesta d'acord amb la realitat de l'Entitat. A banda, es referencia als DS el document RG04-PRDades, l'existència del qual no ha quedat acreditada.

Tanmateix, s'ha constatat que l'Entitat disposa del corresponent registre d'incidències amb els camps exigits per la normativa, tot i afirmar que no han patit incidències de caire greu, com seria la pèrdua de documentació.

Per últim, comentar que mensualment es realitza un informe de revisió del sistema on s'analitzen les incidències patides, tal i com es preveu al punt *5.2.3* dels documents de seguretat (tret del d'administració, que és de nivell bàsic).

Àrees de millora

▲	No detectada	

4.24. Difusió de funcions i obligacions.

Base legal: Article 89.2 RD 1720/2007.

Situació actual

En els documents de seguretat de l'Entitat es fan algunes previsions sobre l'abast del coneixement pel personal de les diferents funcions i obligacions en matèria de protecció de dades, establint que el Responsable del Fitxer vetllarà per a què totes les persones que puguin tenir accés a les dades de caràcter personal tinguin coneixement de l'existència dels documents de seguretat.

D'altra part, en el document *Normes d'Ús* i en el document *Pautes tractaments expedients col·legiats* i el de *Gestió d'expedients* també hi ha indicacions al respecte.

L'Entitat manifesta que està pendent d'aprovació un *Manual d'Acollida*, que fusionarà amb les actuals *Normes d'Ús* per als nous treballadors, que inclourà les funcions i obligacions de tot usuari que tingui accés a dades. Així mateix, els treballadors firmen el compromís de confidencialitat.

El dia 30 de maig va fer difusió entre els treballadors d'una extensa circular informativa LOPD, on informava de tots els extrems relatius a la mateixa, que s'entregava a cada treballador i es feia retornar signada. Aquesta circular conté totes les previsions necessàries sobre LOPD que han de conèixer els treballadors.

L'Entitat manifesta que la setmana anterior als treballs de camp, es va realitzar una sessió de formació en LOPD a tots els treballadors de la casa, amb un nivell d'assistència pràcticament total. Aquest va ser el primer cop que es va donar formació als treballadors en protecció de dades.

Àrees de millora

▲	No detectada	

5. CONCLUSIONS

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-s e valorat la documentació aportada, avaluats els sistemes de tractament de la informació, l'equip auditor detecta que les àrees de millora i salvetats, de conformitat amb l'establert al RDLOPD, són:

ÀREES DE MILLORA
I- BLOC GENERAL
4.1. Auditoria
4.2. Aspectes generals
4.3. Document de seguretat
4.4. Delegació d'autoritzacions
4.5. Tercers (Encarregat de tractament)
4.6. Legitimació de dades
4.7. Drets ARCO
II- BLOC DE MESURES INFORMÀTIQUES
4.12. Identificació i autenticació d'usuaris
III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS
4.21. Entrades i sortides de documents

Barcelona, juny de 2012.

Pere Ruiz Espinós

- Soci -