COL·LEGI OFICIAL D'INFERMERES I INFERMERS DE BARCELONA

INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Número de Protocol 9.827

ÍNDEX

ÍNDEX **2**

1. OBJECTIUS I CONTINGUT **3**

2. METODOLOGIA **4**

3. DADES DE L'ENTITAT I TREBALLS EFECTUATS **5**

3.1. Dades identificatives. *5*
3.2. Treballs efectuats. *6*

4. SIMBOLOGIA **9**

5. ANÀLISI DE LES DIFERENTS ÀREES DE L'AUDITORIA **10**

I - BLOC GENERAL 10
5.1. Auditoria. *10*
5.2. Aspectes generals. *11*
5.3. Document de seguretat. *14*
5.4. Delegació d'autoritzacions. *21*
5.5. Tercers. *22*
5.6. Legitimació de dades. *25*
5.7. Drets ARCO. *28*
II - BLOC DE MESURES INFORMÀTIQUES 29
5.8. Accés a xarxes. *29*
5.9. Connexions remotes. *31*
5.10. Transmissions per xarxes de telecomunicacions. *32*
5.11. Control d'accés. *33*
5.12. Identificació i autenticació d'usuaris. *34*
5.13. Registre d'accessos. *36*
5.14. Còpies de seguretat. *37*
5.15. Fitxers temporals suport automatitzat. *38*
5.16. Registre d'entrades i sortides de suports automatitzats. *39*
III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS 40
5.17. Dispositius portàtils, inventari, etiquetatge, xifrat i destrucció de suports i documents. *40*
5.18. Control d'accés. *41*
5.19. Registre d'accessos. *42*
5.20. Criteris d'arxiu. *43*
5.21. Entrades i sortides de documents. *45*
5.22. Fitxers temporals. *46*
IV- BLOC DE MESURES ORGANITZATIVES 47
5.23. Registre d'incidències. *47*
5.24. Difusió de funcions i obligacions. *48*

6. CONCLUSIONS **49**

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	Q0866003G
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 corporació de dret públic i estructura democràtica al qual han de pertànyer totes les infermeres i infermers que exerceixen la professió en qualsevol de les seves modalitats, amb domicili professional únic o principal dins de la província de Barcelona.

Entre les funcions principals de l'entitat és l'ordenació de l'exercici de la infermeria dins l'àmbit de la seva competència. Així mateix garanteix que l'exercici professional de la infermeria s'adeqüi a la normativa, la deontologia i les bones pràctiques, i que es respectin els drets i els interessos de les persones destinatàries de l'actuació professional.

L' entitat també assumeix la representació corporativa de totes les col·legiats/des davant les autoritat, organismes públics i qualsevol ens legalment constituït.

L'entitat disposa d' Estatuts que regulen el seu funcionament d'acord amb la legislació.

3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els diversos serveis i àrees del Col·legi oficial d'infermeres i infermers de Barcelona.

- Àrea de Sistemes d'Informació i TICs.
- Àrea d' Administració.
- Àrea de Recursos humans i prevenció de riscos laborals.
- Àrea de Col·legiacions
- Àrea de Comunicació i Màrqueting.
- Àrea d' Arxiu.

Pel que fa a espais físics, a més de les àrees indicades, s'han revisat els següents: arxius, despatxos i CPD.

3.2.1. Data de realització de l'auditoria

Dies	6 i 7 de juny de 2016

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 Cazorla	Responsable Comptabilitat i Finances
2	Sra. Núria Garcia Altadill	Adjunta a Gerència i Responsable RRHH (Responsable Protecció de Dades)
3	Sr. Antonio Torrejón Herrera	Director de Sistemes i TICs
4	Sra. Laura Rausell Pastor	Administrativa suport Sistemes i TICs
5	Sra. Montse Téllez Guillén	Administrativa Àrea Gerència (suport societats professionals)
6	Sra. Conxi Lerma Valdivia	Administrativa Formació (suport fitxer Objectores)
7	Sra. Isa Quintana Sánchez	Responsable Atenció Col·legial
8	Sra. Mònica Fidelis Pérez de Tudela	Responsable de Comunicació
9	Sr. Galo Quintanilla Montenegro	Responsable de Màrqueting

10	Sr. Joan Conesa Garrido	Gerent

Relació de la documentació lliurada a l'auditor:

Document
Organigrama
Cartes de l'Agència Espanyola de Protecció de Dades amb els codis d'inscripció dels fitxers
Esquema xarxa informàtica
Procediment del Fitxer activitats de la Fundació
Procediment Fitxer administració
Procediment Fitxer Ciutadans
Procediment Fitxer Client
Procediment Fitxer Col·legiats
Procediment Fitxer Deontologia
Procediment Fitxer Infermeres objectores
Procediment Fitxer Personal
Procediment Fitxer Programa ajuda
Procediment Fitxer Programa CAIIV
Procediment Fitxer Societats Professionals
Procediment Fitxer Voluntari xarxa ciutat refugi
Procediment Fitxer Voluntaris
Registre d'entrades i sortides de documentació dels diferents fitxers
Registre de comprovació *back up*
Recepció CV degut a selecció
Recepció CV espontani
Revisió mensual del sistema
Contractes amb tercers
Formularis exercici drets ARCO
Autorització ús i cessió imatge.

Carta objectores
Cartes resposta de drets ARCO
Document de comprimís de voluntaris
Compromís de Protecció de Dades amb tercers Recerca
Registre Protecció de Dades amb tercers Premis
Consentiment difusió de la pròpia imatge
Consentiment informat comunicació dades de salut laboral
Consentiment infants
Model registre entrada documentació Arxiu General.
Estatus COIB
Organigrama funcional
Manual d'acollida

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. Simbologia

En aquest informe s'hi analitzen tots els punts requerits per la normativa de protecció de dades. En cadascun d'aquests punts s'hi descriu quina és la situació actual, és a dir, la situació en el moment de la realització dels treballs de camp de l'auditoria, i quina és l'àrea de millora o salvetat detectada, que s'il·lustra amb la simbologia següent:

Símbol	Significat
▲	*No detectada*, és a dir, la situació actual de l'Entitat compleix la normativa.
●	*Àrea de millora*, és a dir, l'estat de la situació actual requereix ésser completat perquè no s'ajustaria íntegrament a l'establert a la normativa.
▼	*Salvetat*, és a dir, la situació actual incompleix la normativa i ha de ser modificada de forma prioritària segons les recomanacions efectuades en l'Informe.

5. Anàlisi de les diferents àrees de l'auditoria

I - BLOC GENERAL

5.1. Auditoria.

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

Situació actual

El Col·legi oficial d'infermeres i infermers de Barcelona, en endavant l'Entitat, va realitzar la darrera auditoria en matèria de protecció de dades el juliol de 2014, complint amb les previsions legalment establertes per la legislació en protecció de dades.

L'Entitat ha facilitat el document *Resposta informe 2014* en el que s'indiquen les modificacions efectuades arrel els resultats de la darrera auditoria. L' Entitat afirma, i ha demostrat mitjançant el mostreig, que les conclusions i les accions correctores s'han elevat al representant del responsable del fitxer, que el revisa i aprova.

Àrees de millora

▲	No detectada	

5.2. Aspectes generals.

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

Situació actual

D'acord amb la Llei 7/2006, els Col·legis professionals desenvolupen determinades activitats de naturalesa administrativa i activitats de naturalesa privada. En conseqüència per a l'exercici de les primeres poden utilitzar potestats administratives. Per això, els col·legis professionals, poden ser responsables de fitxers de titularitat pública i també de fitxers de titularitat privada.

Els fitxers que estiguin vinculats a l'exercici de les potestats de dret públic que els atribueix la seva normativa específica seran fitxers de titularitat pública. Mentre que seran de titularitat privada aquells fitxers no vinculats a aquest exercici de potestats de dret públic.

FITXER	CODI	FINALITAT	NIVELL	TRACTAMENT	TITULARITAT
Fitxer de societats professionals inscrites al COIB.	215021002-M	Registre de societats professionals i gestió de les obligacions derivades de la col·legiació; anotació dels socis que integren les societats professionals, de les persones que integren els seus òrgans d'administració i apoderats; modificacions del contracte social, enviament de comunicacions; finalitats històriques i estadístiques.	Bàsic	Mixt	Pública
Col·legiats	204200208-K	Gestió de les prestacions col·legials, representació corporativa, ordenació de l'exercici de la professió.	Mig	Mixt	Pública
Fitxer d'expedients de Deontologia professional, reclamacions, denúncies i queixes, infraccions i sancions	215056030-G	Registre de reclamacions, denúncies o queixes presentades davant actuacions dels professionals col·legiats i de les societats professionals inscrites, control de la seva tramitació i resolució. Control deontològic i disciplinari de l'exercici professional, gestió i	Alt	Mixt	Pública

		tramitació d'expedients disciplinaris i deontològics			
Administració	214000243-C	Realització dels processos habituals de facturació, comptabilitat i financers.	Bàsic	Mixt	Privada
Personal	214000244-K	La gestió de recursos humans a efectes de selecció de personal, contractació i elaboració de nòmines.	Mig	Mixt	Privada
Infermeres objectores al RDL 16/2012	212002265-H	Registre de les col·legiades i col·legiats que manifesten la seva objecció de consciència respecte al RDL 16/2012 i RD 1192/2012, per tal de deixar constància de la seva declaració i als efectes jurídics establerts a l'ordenament jurídic.	Alt	Mixt	Privada
Voluntaris	213001030-X	Recollir les dades dels voluntaris que es presenten a programes de voluntariat del COIB i disposar d'un registre en compliment de l'obligació legal	Bàsic	Mixt	Privada
Ciutadans	214000028-W	Donar opció de consulta i participació al COIB per part dels ciutadans així com atendre queixes i reclamacions	Bàsic	Mixt	Privada
Programa Ajuda	214000245-E	El programa ajuda té l' objectiu de promoure la transformació de la situació de violència de la professional infermera mitjançant accions i estímuls que possibilitin la presa de consciència, autoestima i control sobre la pròpia vida	Alt	Automatitzat	Privada
Programa CAIIV	214000259-Z	Assessorar a les infermeres portadores, afectades per virus transmissibles per sang o que han patit un accident biològic, per tal d'oferir suport i	Alt	Mixt	Privada

		assessorament.			
Voluntaris Professionals Sanitaris per la Xarxa -Ciutat Refugi-	215000276-W	Registre dels professionals sanitaris que vulguin ser voluntaris per donar assistència sanitària als Refugiats i tenir-ho disponible per coordinar-los amb aquelles entitats i institucions que ho demanin.	Mig	Automatitzat	Privada
Inscripció no col·legiats	21202264-V	Donar serveis d'assessories del SBDI, d'esdeveniments entre d'altres serveis del Col·legi.	Bàsic	Mixt	Privada

Salvetat

▼	Salvetat	L' Entitat, a part dels declarats en el quadre superior, té declarats a l' Agència Española de Protecció de Dades, pel que fa a titularitat pública, el fitxer de col·legiats, el fitxer d'expedients de deontologia professional reclamacions, denúncies i queixes, infraccions i sancions, el fitxer de societats professionals inscrites al col·legi oficial d'infermeres i infermers de Barcelona. Pel que fa a la titularitat privada té declarats el fitxer d'administració, el fitxer de personal, el fitxer de ciutadans, el fitxer d'inscripció no col·legiats, el fitxer objectores al RDL 16/2012, el fitxer de programa d'ajuda, el fitxer del CAIIV, el fitxer de voluntaris, i el fitxer de voluntaris professionals sanitaris per la xarxa ciutat refugi.

5.3. 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 (DS) 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 únic document de seguretat que inclou tots els fitxers declarats per l' Entitat. • Hi ha elaborats els documents "Procediments" per cada un dels fitxers inscrits. En els quals s' específica allò establert en el DS per cada fitxer.
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: • L' Entitat disposa d'un inventari de suports. • En el punt 1 del DS consta una descripció dels fitxers. Així mateix, en l' Annex B hi consta la descripció de l'estructura física dels fitxers, detallant les dades recollides en cadascun dels fitxers.

- La descripció dels sistemes d'informació la trobem en l' Annex C.

- Hi consta també en el punt 5.2 *Estructura del fitxer i descripció del suport informàtic amb el que està tractat* dels documents de procediments de cadascun dels fitxers.

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)*.

Comentari:

- No aplica.

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

Comentaris:

- L'entitat disposa de documents de *Procediments* per a cadascun dels fitxers.

- L'Entitat té elaborats diferents annexes i procediments.

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

Comentari:

- En el punt 5 del DS es regulen els funcions i obligacions del personal. Així mateix punt 5.4 del document de procediments també s'hi troba un manual de funcions.

- Annexat al DS (annex H) s'hi detallen les funcions i obligacions de l'encarregat intern del tractament, del responsable de seguretat, dels usuaris i dels

administradors o del personal informàtic.

- També consta un document d' informació i compromís de confidencialitat, anomenat *Registre d' Informació i compromís en quant al deure de confidencialitat.*

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

Comentari:

- La notificació i la gestió de les incidències consta en l' annex I " *Notificació i Gestió d'incidències*". Disposen del model de registre d'incidències.
- En el punt 5.4.6 i 5.4.7 dels documents de procediments també es regula el registre d'incidències.

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

Comentari:

- Es troba regulat en el punt 10 del DS i en l' annex G3, *Procediment de suport i recuperació.*
- En el document de procediments s'hi estableix el procediment, periodicitat i custòdia per a la realització de còpies de seguretat.

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.

Comentaris:

- Pel que fa al transport de suports es regula en el punt 8.1.6 del DS. Tot i així, l' Entitat cal que amplïi aquest punt. Consta que l' Entitat ho ha realitzat desprès de realitzar l'auditoria.
- L'Entitat estableix la destrucció de suports en el punt 8.2.3 del DS. Es disposa de l' annex G.6 *Procediment per a la destrucció de rebuigs informàtics*.

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.
Comentaris: • L'entitat disposa de llistats on consten tots els tercers encarregats de tractament.
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.
Comentari: • No consten en el llistat citat a l'apartat anterior.
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.
Comentari: • En el punt G7 de l' annex G "*Procediment de control i seguretat*" es regulen les autoritzacions per a l'ús de PC portàtils i dispositius mòbils.
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 ho preveu a l' Annex G.7 del DS. No consta el període de validesa. Ens informen que s'ha incorporat el període de validesa de manera posterior a

l' Auditoria.
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.
Comentaris: • S'estableix en l' annex G1, *Instruccions per donar altes, baixes o modificacions d'accés d'Usuaris.*
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: • Aquests consten en els punts *Control i limitació d'accés físic*, apartat "a", dels DS.
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: • En l'Annex F s'inclou la relació d'usuaris actualitzada amb accés autoritzat a cada sistema d'informació que tingui accés a les dades dels Fitxers • A l' annex E s'estableix el registre d'accessos als diferents espais on s'hi troben suports i documents. • També en el punt 5.4.5 del document de procediments es troben regulats els controls de limitació física. • En el punt 6.1 del DS s'estableix l' autorització del personal que pot accedir als fitxers.
P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.
Comentaris: • En l' annex G, i concretament en el punt G.5 Procediment de gestió i sortida de suports, es detallen les persones autoritzades per l'entrada i suports de correus electrònics. També es preveu en l' annex F.

Q. Personal autoritzat per a la recepció/ enviament de dades de caràcter personal *(nivell mitjà i/ o alt).*
Comentari: • Esta previst en l' annex G5 i a l'annex F.
R. Personal autoritzat per a la realització del procediment de recuperació de dades.
Comentari: • Es fa esmenten el punt 10 del DS.
S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.
Comentaris: • Aquests es troben en l' annex F *Nomenaments i autoritzacions.* Tot i així durant el DS i els documents de Procediments de cadascun dels fitxers es van realitzant delegacions per part del responsable del fitxer.
Altres mesures
T. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat.
Comentari: • Consta en l' annex G.2 *Instruccions de control d'identificació i autenticació* del DS el procediment d'assignació, distribució i emmagatzematge de contrasenyes.
U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.

Comentari: • Consta en l' annex G.2 *Instruccions de control d'identificació i autenticació* DS el procediment d'assignació, distribució i emmagatzematge de contrasenyes.
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.
Comentari: • No consta que a dia d'avui es realitzin proves amb dades reals.
W. Identificació del responsable de seguretat *(nivell mitjà i/ o alt).*
Comentari: • Queda determinat en el punt 5.4.2 dels documents de Procediment.
X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt).*
Comentari: • L' Entitat estableix en l' annex J *Controls periòdics mensuals* els controls necessaris per verificar el compliment del que disposa el document, així com les auditories.

Àrees de millora

●	Àrea de millora	Cal que s'acabin de detallar els punts comentats en el quadre anterior.

5.4. Delegació d'autoritzacions.

Base legal: Article 84 RD 1720/2007.

Situació actual

Les autoritzacions que s'atribueixen al responsable del fitxer poden ser delegades en les persones designades en aquest efecte. Es duen a terme delegacions per part del responsable del fitxer durant el transcurs del Document de Seguretat i dels documents de Procediments de cadascun dels fitxers inscrits.

Àrees de millora

▲	No detectada	

5.5. Tercers.

ENCARREGATS DE TRACTAMENT

Base legal: Article 82 RD 1720/2007.

Situació actual

L' Entitat disposa d'un llistat on s'estableix l'encarregat de tractament, els fitxers a tractar, el servei prestat, data del contracte i persona responsable.

De la documentació aportada per l' Entitat, es realitza el mostreig del qual es comenta el següent:

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
Plataforma de Organización Logística	Servei mailing	☒	El contracte aportat no dóna compliment a l'article 12 LOPD, ja que manca identificar i detallar les mesures de seguretat que l'encarregat de tractament ha d'aplicar.
Salvetti & Llombart, S.L.	Estudis de mercat	☒	El contracte aportat no inclou una clàusula que doni compliment a l'article 12 LOPD.
Denver Advocats i Assesors Ttributaris, S.L.P	Assessorament jurídic i fiscal	☒	El contracte aportat no inclou una clàusula que doni compliment a l'article 12 LOPD.
ALFA Enginyers informàtics, S.L.	Manteniment de A3 ERP	☑	Disposen de contracte d'acord amb les previsions de l'art. 12 LOPD.
Isabel Pera	Assessorament	☒	El contracte aportat no dona compliment a l'article 12 LOPD, ja que manca identificar i detallar les mesures de seguretat que l'encarregat de tractament ha d'aplicar.

Salvetat

▼	Salvetat	Cal firmar un contracte d'encarregat de tractament amb tots els tercers que per la prestació o objecte del conveni hagin de tenir accés a dades de caràcter personal dels fitxers de l'entitat. És necessari que en el contracte d'encarregat de tractament s'estipulin les mesures de seguretat que aquest ha d'implementar.

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

Del mostreig efectuat en destaquem els següents tercers sense accés a dades:

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS	COMENTARIS
UNIPOST	Serveis d'enviament de documentació		
Integral Facility Seven , S.L	Neteja	☑	Disposen de contracte d'acord l'establert en la normativa.
SISTEMAS DIGITALES CORPORATE, S.L	Manteniment equips multifunció	☒	Si bé consta una clàusula de confidencialitat no s'hi fa menció a la prohibició expressa d'accedir a dades de caràcter personal.

Àrees de millora

●	Àrea de millora	Veure el quadre anterior.

5.6. Legitimació de dades.

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

Situació actual

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

FITXER	LEGITIMACIÓ	COMENTARIS
Col·legiats	Es fa entrega de document d'informació i consentiment en el cas de noves col·legiacions.	Aquesta document és suficient en els termes requerits per la norma.
Voluntariat	L' Entitat fa entrega als voluntaris del document "Document de Compromís-Voluntariat COIB".	Cal informar de la recollida de dades d'acord amb l'article 5 LOPD, pel que s'ha d'incloure una clàusula en el document en referència al tractament de dades.
Recerca	Revisió del document "Compromís de protecció de dades amb tercers Recerca".	Manca informar de la identitat del responsable del tractament.
Premis COIB	Revisió del document "Protecció de dades amb tercers premis".	Manca informar de la identitat del responsable del tractament, així com de l'existència d'un fitxer del qual es titular el COIB.
Personal	El contracte laboral incorpora una clàusula addicional tercera sobre Protecció de dades.	Aquesta clàusula és suficient en els termes requerits per la norma.
	Es fa entrega als nous treballadors del document "Consentiment Difusió de la pròpia imatge".	Aquest document és suficient en els termes requerits per la norma.

	L'entitat entrega un document com a resposta a la recepció de CV durant un procés de selecció.	Aquest document és suficient en els termes requerits per la norma.
	L'entitat entrega un document com a resposta a la recepció de CV rebut de manera espontània.	Aquest document és suficient en els termes requerits per la norma.
Ciutadans	A la web existeixen formularis per sol·licitar informació varia.	Aquest document és suficient en els termes requerits per la norma.
Queixes i suggeriments	A la web existeixen formularis per enviar missatges al COIB, en forma de queixes i suggeriments.	Aquest document és suficient en els termes requerits per la norma.
Cessió d'imatges	L' Entitat fa entrega als participants en ponències, cursos, activitats, etc. del document "Cessió drets imatge".	Aquest document no és suficient en els termes requerits per la norma. Cal informar de l'existència d'un fitxer i del responsable del tractament.
	Existeix un document d' autorització de cessió d'imatges d'infants.	Aquest document és suficient en els termes requerits per la norma. Cal informar de l'existència del fitxer així com el responsable del tractament.
Formulari Xarxa Ciutat Refugi	Està disponible un formulari a la web.	Aquest document és suficient en els termes requerits per la norma
Newsletter	Incorpora una clàusula relativa a protecció de dades.	Aquest document és suficient en els termes requerits per la norma.
Infermeres objectores	Les infermeres han d'omplir i entregar un model de carta del COIB.	Aquest document és suficient en els termes requerits per la norma.

Salvetat

▼	Salvetat	Els titulars de les dades de caràcter personal les quals es sol·liciten han de ser informats de manera expressa, precisa i inequívoca de l'existència d'un fitxer, de la finalitat de la recollida de les seves dades i dels destinataris de la informació, del caràcter facultatiu o no de les seves respostes, de les conseqüències de l'obtenció de les dades, de la possibilitat d'exercir els seus drets arco, així com la identitat i direcció del responsable del tractament. Es recomana informar sobre el nom del fitxer proporcionant així més informació al titular de les dades i complir amb major grau amb la normativa i amb els principis orientadors de protecció de dades de caràcter personal.

5.7. Drets ARCO.

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

Situació actual

El procediment per a l'exercici dels drets ARCO està descrit en el punt 12 del DS. L' Entitat disposa de models d'exercici del dret d'accés, rectificació, cancel·lació i oposició. Així mateix consten com a annex (annex L) les cartes de respostes a l'exercici per cadascun dels drets ARCO, com també la carta refusant l'exercici dels drets ARCO.

Pel que fa als terminis, el DS estableix que pel que fa a drets d'accés, un cop comprovada la sol·licitud d'exercici l' Entitat notificarà la informació a l'interessat en el termini màxim d'un mes des de la presentació de la sol·licitud. Pel que fa al dret de rectificació i cancel·lació l' Entitat notificarà l' efectivitat de l'exercici del dret en el termini de deu dies des de la data de la presentació de la sol·licitud.

Durant els treballs de camp l' Entitat afirma que no s'ha exercit cap dret ARCO des de l' última auditoria.

Àrees de millora

▲	No detectada	

II - BLOC DE MESURES INFORMÀTIQUES

5.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'Entitat disposa del mapa del diagrama de xarxa (annex D2), així mateix es realitza una descripció dels servidors i de l'entorn del sistema operatiu en l' annex D1 del DS. A l' annex D2 també es troba una explicació sobre l' entorn de comunicacions i de la xarxa cablejada.

Pel que fa a l'accés a les dades s'utilitza una xarxa interna LAN, que enllaça a tots els equips informàtics per fibra òptica. Hi ha connexions WIFI però es troben aïllades de la xarxa de l' Entitat.

Disposen d'un *rack* a la planta baixa, i dos switch a la primera planta i un a la tercera planta, utilitzant enllaços de fibra òptica.

En quant a les mesures de seguretat, els treballadors es connecten a internet a través d'un Firewall. L' Entitat disposa d'un antivirus, *Eset*.

L'Entitat disposa d'un SAI (sistema d'alimentació ininterromput), per tal de donar resposta en cas de fallida d'electricitat.

Pel que fa als servidors l'Entitat disposa d'un servidor físic i tres servidors virtuals.

A part d'això hi ha un sistema de servidors en el cloud de "AZURE Microsoft". En aquests servidors es troba el programa de gestió dels col·legiats, Ulisses.

Els treballadors i col·legiats disposen de correu electrònic (Office 365). Aquests correus electrònics són individuals.

Pel que fa al sistema de carpetes, l'Entitat presenta un sistema de carpetes en xarxa departamentals. L' accés a les carpetes és limitat segons la categoria professional, limitant-se l'accés al personal de cada Departament o per serveis. També hi trobem carpetes en xarxa personals dels professionals.

Les principals aplicacions que tracten dades de caràcter personal són els següents:

APLICACIÓ	UTILITAT
Ulisses	Gestió col·legial
A3	Comptabilitat

IMAGIC	Biblioteca i arxiu
WEB PUBLISHER	Biblioteca i arxiu
ANSWER	Biblioteca i arxiu
TOT	Biblioteca i arxiu
MAGIC INFO	Gestor documental i de biblioteca
INOLOGY	Control de presència
TARIFICADOR	Control de trucades
FILE AUDIT	Accessos al directori actiu

Àrees de millora

▲	No detectada	

5.9. Connexions remotes.

Base legal: Article 86 RD 1720/2007.

Situació actual

En el *punt 6.4 Llocs de treball* del DS s'hi regula les accions remotes. L' annex D2 *Entorn de xarxes* s'hi dedica un apartat a detallar com són les connexions remotes. Així mateix en l'annex G7 hi consta el llistat de persones amb accés VPN.

L'Entitat informa que es produeixen tractaments de dades fora dels locals on es troben ubicats els fitxers. Des de l' Entitat s' estableix que els membres de juntes i responsables d' àrees poden accedir remotament.

Per accedir remotament s'ha d'introduir el mateix nom d'usuari que tenen per accedir al sistema i un *password*.

En el cas que algun treballador hagi d'accedir remotament s'ha de demanar autorització a sistemes d'informació, que permet una connexió VPN facilitant l'accés des del Firewall.

Hi ha empreses externes amb accés remot, tal i com s'estableix en el DS.

Es pot afirmar que les mesures de seguretat emprades per al treball fora del lloc on s'ubiquen els fitxers garanteixen el nivell de seguretat corresponent al tipus de fitxer tractat.

Àrees de millora

▲	No detectada	

5.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

L' entitat regula les transmissions per xarxes de telecomunicacions en el punt 9 del DS, en el qual s'estableix que únicament es faran entrades i sortides per correu electrònic des del compte de correu electrònic d'usuaris autoritzats. Així mateix es determina que es guardaran còpia dels correus electrònics en directoris protegits que signifiquin entrades o sortides de dades. En l' annex F es detallen les persones autoritzades, així com una còpia dels fitxers rebuts o transmesos per sistemes de transferència per xarxa.

Actualment l'entitat utilitza un sistema de transmissió de la informació sense programa de xifratge. S' utilitzen les eines de Microsoft 365.

Des del Departament de Sistemes d'Informació apuntaren que l'ús d'aquestes eines és bastant residual, atès que no es generen comunicacions amb dades de salut.

L' àrea de recursos humans van afirmar que quan es realitza una nova contractació l' Entitat envia el DNI, número de seguretat social i número de compte a Solfico a través de correu electrònic.

Durant els treballs de camp, l' àrea de col·legiacions va comentar que es realitzen documents excels amb les altes i baixes col·legials. Aquests documents s'envia a l'asseguradora i al "manipulador".

Afirmaren que no s'utilitza el fax per l'enviament de documentació. Així mateix estan estudiant la possibilitat d'eliminar la possibilitat rebre faxos.

Àrees de millora

●	Àrea de millora	Tots els enviaments externs de documentació amb dades de nivell alt mitjançant el correu electrònic s'han de realitzar amb un mecanisme de xifratge suficientment segur (veure Dictamen CNS12/2013 de l'APDCAT), no essent suficient un arxiu amb contrasenya ni qualsevol versió dels programes .zip o .rar.

5.11. Control d'accés.

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

Situació actual

L' Entitat estableix de forma extensa i detallada el procediment per donar d'alta, baixa o modificar l'accés d'usuaris en l' annex G, concretament al punt G1.

En el mateix annex comentat es determina que es comprovarà que la llista d'usuaris autoritzats en les aplicacions de l' Entitat és correcta i que es fidel a la realitat. Es pot observar un llistat amb el noms i els usuaris amb accés.

Durant els treballs de camp se'ns informa que pel que fa a les altes, quan hi ha una nova contractació l' àrea de recursos humans comunica per correu electrònic al departament d'informàtica indicant els permisos i accessos. El procediment per modificacions i baixes és el mateix, i són immediates.

El programa de gestió col·legial té diferents mòduls i no tothom te accés a tots ells, per aquest motiu recursos humans informa dels permisos quan es realitza una alta. Així mateix s'adjunta en l' annex F els permisos per usuari dins del programa Ulisses.

Els mecanismes que impedeixen que els usuaris accedeixin a més dades de les autoritzades és l'ús de contrasenyes.

Àrees de millora

▲	No detectada	

5.12. Identificació i autenticació d'usuaris.

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

Situació actual

L' Entitat estableix en el punt 6.2 del DS el procediment d'identificació i autenticació d'usuaris. Així mateix en l' annex G es troba descrit el procediment d'assignació, distribució i emmagatzematge de contrasenyes. En els documents de Procediments també es fa referència.

Tot el personal amb accés al sistema i als programes disposa d'usuari i contrasenya, de manera que es garanteix la correcta identificació i autenticació dels usuaris.

La identificació de qualsevol usuari per accedir al sistema i als programes és inequívoca i personalitzada.

En relació al sistema la contrasenya és de 6 dígits i ha de ser diferent al nom d'usuari (inicial del nom seguit del cognom). Les contrasenyes caduquen cada quatre mesos. A l' hora d'establir la nova contrasenya no es poden repetir les contrasenyes dels tres últims mesos. Es realitza el bloqueig al tercer intent erroni. També es produeix bloqueig per desús de l'equip de més de 10 minuts.

Pel que fa a l' Ulisses tot el personal té usuari i contrasenya. El primer cop que es proporciona una contrasenya s'ha de canviar. La contrasenya és de 6 dígits i no hi ha l'obligació de que sigui alfanumèrica. Existeix bloqueig per desús als 5-10 minuts. També es bloqueja al tercer intent erroni. La contrasenya no caduca. Segons s'informa les contrasenyes s'emmagatzemen de forma inintel·ligible.

El procediment d'assignació, distribució i emmagatzematge de la contrasenya per accedir al sistema i a les aplicacions garanteix la seva confidencialitat i integritat. Mentre estan vigents, les passwords s'emmagatzemen de forma inintel·ligible, a excepció de la contrasenya del xHIS.

Àrea de millora

●	Àrea de millora	Les contrasenyes han de tenir caducitat, com a mínim una vegada cada 12 mesos. Les contrasenyes s'han d'emmagatzemar de forma inintel·ligible. Es recomana seguir aquestes directrius, per definir les contrasenyes com a segures: • No contenir el nom d'usuari ni parts del nom complet d'usuari en més de dos caràcters consecutius. • Tenir una longitud mínima de vuit caràcters. • Incloure caràcter de tres de les següents categories: majúscules, minúscules , dígits de base 10 , caràcters no

		alfanumèrics (per exemple: !, &, #, +...) • No repetir contrasenya anterior. • Periodicitat de canvi, mínim cada 6 mesos. • Bloqueig al tercer intent erroni de validar-se al sistema. Bloqueig en cas de desús per part de l'usuari (5-10 minuts), per tal de que es requereixi la introducció de nou dels noms d'usuari i claus de pas per a reiniciar l'activitat en aquells equips que tinguin accés a dades personals

5.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

Durant els treballs de camp s'informa que gerència i el cap de sistemes informàtics reben un correu electrònic que proporciona l'eina FileAudit on es llista els usuaris que han accedit o que han intentat accedir, fent constar l'usuari, la data i si l'accés ha estat autoritzat o denegat.

Es comunica que setmanalment es revisen els accessos, però no queda constància que s'elabori el preceptiu informe.

Àrea de millora

●	Àrea de millora	Cal que el responsable de seguretat a més de revisar els accessos un cop al mes la informació del control registrada, elabori un informi de les revisions realitzades i els problemes detectats.

5.14. Còpies de seguretat.

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

Situació actual

En el punt 10 del DS hi trobem regulats el procediment de suport i recuperació i en el punt 11 els control periòdics de verificació del compliment. Així mateix en l' annex G3 s'estableix de la instrucció de suports i recuperació, explicant detalladament la realització de les còpies de seguretat.

Durant els treballs de camp s'informa que diàriament es realitzen dues còpies, una a les 13:30 hores i una altra a les 21:00. Cada divendres es fan còpies setmanals en cintes. Cada mes també es fan còpies en cinta.

Mensualment es canvia la cinta per una que es troba en una caixa ignífuga i la que s'extreu es porta a la caixa forta del banc.

Pel que fa a la verificació de les còpies es comenta que l'administrador és capaç de verificar si les dades s'han gravat correctament.

S'afirma que es realitzen recuperacions de dades i que aquestes queden registrades en un full de còpies de *backup*. La persona que sol·licita la recuperació de les dades verifica que s'hagi realitzat correctament. S'ha fet entrega del mostreig referent al registre de comprovació de *backup*.

No es realitzen proves en dades reals.

Àrees de millora

▲	No detectada	

5.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

En el punt 6.7 "*Bases de dades, fitxers o arxius ofimàtics*" del DS, es regulen els fitxers temporals. En aquest queda expressament prohibit el tractament de dades amb programes ofimàtics, processadors de textos i fulls de càlcul sense comunicació prèvia al Responsable de Seguretat. Així mateix es recomana evitar guardar còpies de dades en arxius temporals, que en el cas que sigui imprescindible s'haurà d'efectuar les còpies sobre un mateix directori, eliminar-se quan siguin innecessàries, i complir amb el nivell de seguretat que els hi correspongui.

Durant els treballs de camp es comunica que tots els documents que realitzen els treballadors han de quedar guardats a la xarxa.

Àrees de millora

▲	No detectada	

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

Base legal: Article 97 RD 1720/ 2007.

Situació actual

En el punt G5 de l' annex G " *Procediment de control i seguretat*" del DS es regula el procediment de gestió d'entrada i sortida de suports, en el qual es determina la persona responsable de les entrades sortides de cintes de *backup*. S'adjunta a l'annex un registre de sortida on es pot observar la data, qui efectua el trasllat, la ubicació (banc, caixa forta, unitat robòtica), número de cinta i observacions. També s'adjunta un registre d'entrada de suports en el que queda constància del tipus de suport, data, hora d'entrada, receptor, contingut i motius.

L'única sortida de suports que es preveu i que es determina durant els treballs de camp és la de cintes en les quals es realitzen les còpies de *backup,* de les quals s'aporta mostreig del registre. L'Entitat disposa com a registre d'aquests moviments els rebuts que facilita el banc cada cop que es guarden i/o es retiren les còpies de seguretat emmagatzemades a la caixa forta.

Àrees de millora

▲	No detectada	

III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS

5.17. 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 punt G7 de l' annex G "*Procediment de control i seguretat*" es regulen les autoritzacions per a l'ús de PC portàtils i dispositius mòbils. Es comentà que existeix inventari de suports fent entrega d'un mostreig d'aquest.

Únicament els membres de la Junta de Govern, Gerent, Direcció de Programes, secretaries i responsables de departaments disposen de portàtils. Pel que fa a *smartphones* l' Entitat afirma que existeixen però que aquests no tenen accés a la xarxa, encara que sí al correu electrònic.

Tot i que els ports USB dels equips estan habilitats, afirmaren que s'utilitzen encara que des de la corporació no es faciliten.

La reparació dels equips i discs durs es realitza de manera interna, *in situ*, pel personal del departament d'Informàtica.

La destrucció del suport paper amb dades de caràcter personal s'efectua mitjançant destructores ja que, segons ens informen, es disposa d'una a cada departament.

Actualment no es porta a terme la destrucció d'equips informàtics, ja que aquests s'emmagatzemen en la sala de servidors. Pel que fa als discs durs aquests els destrueix una empresa externa que aporta un certificat.

Les cintes amb les quals es fan les còpies de seguretat estan degudament etiquetades a la caixa forta que es troba a la sala de servidors.

Àrees de millora

▲	No detectada	

5.18. Control d'accés.

Base legal: Articles 99, 107, 108 i 111 RD 1720/ 2007.

Situació actual

En l' annex E "*Locals i equipaments*" es detalla el control d'accessos a diferents punts de l' Entitat. En aquest punt també trobem detallats els mecanismes de tancament dels dispositius d'emmagatzematge.

El centre de l' Entitat es troba en un edifici que comparteix amb empreses i altres entitats. Per accedir a algunes parts de l' Entitat des de dins de l'edifici s'ha de disposar d'una targeta d'accés.

L' annex E estableix que a la sala d'expedients col·legials te accés tot el personal d'Atenció i Administració Col·legial, el Responsable de Manteniment i l' Adjunta a Gerència. La clau es troba en un armari tancat en clau que es troba a la recepció de la planta baixa de l' Entitat. Durant els treballs de camp es va poder comprovar que es portava a terme un registre d'accessos a aquesta sala.

Pel que fa a dispositius d'emmagatzematge com armaris i arxivadors tots disposen de mecanisme de tancament. Durant els treballs de camp es va poder comprovar que aquests restaven tancats.

La documentació que no està arxivada per motius de treball ja que ha de ser signada per la Secretaria de Junta, com per exemple els expedients de noves col·legiacions i expedients de trasllats, es troben en una safata en un armari.

La sala on es troben els servidors està tancada en clau, aquesta clau sempre la té l' administrativa de suports TIC. En l'annex E consten les persones autoritzades per accedir-hi (Responsable de suport informàtic, el Responsable de manteniment, l' Adjunta a Gerència i el Director de Sistemes i TICs), així mateix queden determinades les empreses de manteniment que tenen accés a la sala de servidors. Durant la reunió se'ns informa que el personal de manteniment ha d'accedir acompanyat per la administrativa de suport informàtic.

Mitjançant el mecanisme de control d'accessos es garanteix que només el personal autoritzat te accés als llocs on es troben instal·lats els equips físics que donen suport als sistemes d'informació.

Àrees de millora

▲	No detectada	

5.19. Registre d'accessos.

Base legal: Article 113 RD 1720/2007.

Situació actual

L'Entitat fa menció als registres d'accessos a l' annex E del DS. També s'adjunten models de registre d'accessos.

Tal com s'ha indicat en el punt anterior l'accés a l' Entitat des de l' edifici es fa mitjançant targetes d'accés. Aquests accessos queden guardats en el programa "Control de Terminales", el qual permet extreure els accessos que s'han produït per persona i dia.

Pel que fa a la sala d'expedients col·legials a l' annex mencionat s'adjunta el model de registre d'accessos on queda constància de la data, hora, persona, motiu i hora de retorn.

Àrees de millora

▲	No detectada	

5.20. Criteris d'arxiu.

Base legal: Articles 106 RD 1720/2007.

Situació actual

En els punts 5.2 del document de procediments de cada fitxer està descrita l' estructura d'aquest.

Durant l'anàlisi dels treballs de camp s'estableix el següent:

Pel que fa al fitxer de col·legiats l' Entitat disposa de la sala d'expedients col·legials. Es troba situada a la planta baixa. Aquest té les funcions d'arxiu actiu i passiu, ja que es troben els expedients actuals i els històrics. Els expedients estan ordenats per número d'expedients de manera seqüencial. En el document de procediments del fitxer de col·legiats es descriu en el punt 5.2 l' estructura del fitxer. Si bé es comprovà que l'arxiu es troba sota la custòdia de l'àrea de col·legiacions, no consta el responsable de l'arxiu.

El departament d' administració disposa d'arxiu actiu i passiu. En l'actiu es troben les factures en paper de l'exercici en curs i de l' exercici anterior que es guarden en dos armaris que es tanquen en clau a l' àrea de comptabilitat. A l' arxiu passiu, que és el general, es troba la documentació de la resta d'anys. S' informa que del arxiu passiu encara no s'ha destruït res. En el document de procediments del fitxer d'administració es descriu en el punt 5.2 l' estructura del fitxer. No consta el responsable de l'arxiu però com s'ha indicat pel fitxer de col·legiats, el responsable de l'arxiu és l'àrea de col·legiacions.

La documentació amb dades de caràcter personal referent a infermeres objectores resta emmagatzemada en un *book* amb tancament amb clau, situat a l' àrea de formació. En el document de procediments del fitxer d' infermeres objectores es descriu en el punt 5.2 l' estructura del fitxer. No consta el responsable de l'arxiu.

El departament de recursos humans disposa d'arxiu actiu i passiu. La documentació que forma l'arxiu actiu es troba en un armari situat al despatx de gerència i resta ordenada per codi d'alta. Quan es rescindeix el contracte del treballador el seu expedient passa a l'arxiu passiu que es troba en armaris situats als despatx del departament, del qual encara no s'ha destruït documentació. En el document de procediments del fitxer de personal es descriu en el punt 5.2 l' estructura del fitxer. La responsable de l'arxiu és la responsable de RRHH de l'Entitat.

El departament de societats professionals disposa d'un arxiu actiu on es guarden les cartes i documentació referent. La documentació es guarda en un armari tancat amb clau i està ordenada per codi de societats professionals. No disposen d'arxiu passiu ni, ens comenten, tampoc s'ha destruït documentació.

Els criteris d'arxiu descrits podem considerar que garanteixen la correcta conservació dels documents, la localització i la consulta de la informació i l'exercici dels drets ARCO.

Àrees de millora

▲	No detectada	

5.21. Entrades i sortides de documents.

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

Situació actual

Dels moviments de documentació que surt dels arxius actius i passa als arxius passius queda constància en un registre d'entrada i sortida de documentació.

El departament d'administració ens informa que disposa de registre d'entrada i sortida de documentació que rep mitjançant correu electrònic.

Pel que fa a les cartes d' infermeres objectores també es disposa registre d'entrada d'aquesta documentació.

El departament de recursos humans quan hi ha una nova contractació envia a Solfico mitjançant correu electrònic el DNI, el número de seguretat social i el número de compte. També es realitzen enviament a la empresa que s'encarrega de la formació i al Fremap. Segons ens informen, aquestes sortides queden registrades.

Àrees de millora

▲	No detectada	

5.22. Fitxers temporals.

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

Situació actual

Durant els treballs de camp s'observà que en els diferents departaments no es treballa de forma generalitzada amb fitxers temporals.

Àrees de millora

▲	No detectada	

IV- BLOC DE MESURES ORGANITZATIVES

5.23. Registre d'incidències.

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

Situació actual

En els DS consta el punt 7 on es regula la gestió d'incidències, en el qual es fa menció al registre d'incidències. En l'annex *Notificació i Gestió de les incidències* s'adjunta el model de registre d'incidències, del qual l' Entitat aporta un mostreig.

La persona que detecta una incidència ho comunica telefònicament o per correu electrònic a l'administrativa de suports TIC. Seguidament es fa constar en el registre d'incidències, en el qual es detalla: data i hora en què es va produir, persona que realitza la notificació, persona a qui es comunica, descripció de l' incidència, efectes que pot produir, solució presa, data en què s'adopta la solució, responsable de la solució, resultat de l'acció presa i data de tancament.

Hi ha dues empreses externes de manteniment informàtic que donen suport en la gestió de les incidències: Kahuna i Sofiteg.

Àrees de millora

▲	No detectada	

5.24. Difusió de funcions i obligacions.

Base legal: Article 89.2 RD 1720/2007.

Situació actual

Quan es dóna una nova incorporació es fa entrega del compromís de confidencialitat i del manual d'acollida en relació a les funcions i obligacions. El manual d'acollida determina algunes obligacions en matèria de protecció de dades de manera genèrica. D'altra banda, es troba a faltar la determinació de les conseqüències en cas d'incompliment per part dels treballadors de les obligacions que li son pròpies en matèria de protecció de dades.

En el document "Resposta informe 2014" es fa constar que es va enviar una circular al personal informant sobre el DS.

Segons s'indicà durant els treballs de camp, d'ençà la darrera auditoria no s'ha procedit a fer formació en matèria de protecció de dades.

Àrea de millora

●	Àrea de millora	Cal fer una major difusió de les funcions i obligacions en matèria de protecció de dades tot incorporant al manual d'acollida les conseqüències en cas d'incompliment de les funcions que li són pròpies. Cal que l'Entitat desenvolupi formació en matèria de protecció de dades de manera periòdica.

6. 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-se 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
5.3. Document de seguretat
5.5 Tercers
II- BLOC DE MESURES INFORMÀTIQUES
5.10. Transmissions per xarxes de telecomunicacions
5.12. Identificació i autenticació d'usuaris
5.13. Registre d'accessos
IV- BLOC DE MESURES ORGANITZATIVES
5.24. Funcions i obligacions

SALVETATS
I- BLOC GENERAL
5.2 Aspectes generals
5.5. Tercers (Encarregats de tractament)
5.6. Legitimació de dades

Barcelona, 30 de juny de 2016.

Pere Ruiz Espinós

- Soci-