

COL·LEGI OFICIAL D'INFERMERES I INFERMERS DE BARCELONA
INFORME D'AUDITORIA DE PROTECCIÓ DE
DADES DE CARÀCTER PERSONAL

Número de protocol 8.783

ÍNDEX

ÍNDEX	2
1. OBJECTIUS I CONTINGUT.....	3
2. METODOLOGIA	4
3. SIMBOLOGIA.....	5
4. DADES DE L'ENTITAT I TREBALLS EFECTUATS	6
4.1. Dades identificatives.....	6
4.2. Treballs efectuats.....	7
5. ANÀLISI DE LES DIFERENTS ÀREES DE L'AUDITORIA	11
I - BLOC GENERAL.....	11
5.1. Auditoria.....	11
5.2. Aspectes generals.....	12
5.3. Document de seguretat.....	15
5.4. Delegació d'autoritacions.....	21
5.5. Tercers.....	22
5.6. Legitimació de dades.....	24
5.7. Drets ARCO.....	28
II - BLOC DE MESURES INFORMÀTIQUES	29
5.8. Accés a xarxes.....	29
5.9. Connexions remotes.....	30
5.10. Transmissions per xarxes de telecomunicacions.....	31
5.11. Control d'accés.....	32
5.12. Identificació i autenticació d'usuaris.....	33
5.13. Registre d'accessos.....	34
5.14. Còpies de seguretat.....	35
5.15. Fitxers temporals suport automatitzat.....	36
5.16. Registre d'entrades i sortides de suports automatitzats.....	37
III- BLOC DE MESURES FÍSQUES O DOCUMENTALS.....	38
5.17. Dispositius portàtils, inventari, etiquetatge, xifrat i destrucció de suports i documents.....	38
5.18. Control d'accés.....	39
5.19. Registre d'accessos.....	40
5.20. Criteris d'arxiu.....	41
5.21. Entrades i sortides de documents.....	43
5.22. Fitxers temporals.....	44
IV- BLOC DE MESURES ORGANITZATIVES.....	45
5.23. Registre d'incidències.....	45
5.24. Difusió de funcions i obligacions.....	46
6. CONCLUSIONS.....	47

I. Objectius i contingut

De conformitat amb el que estableix la normativa vigent sobre protecció de dades¹, 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 dur a terme l'auditoria s'ha realitzat una revisió in situ de les instal·lacions de tractament de dades i de sistemes d'informació de l'entitat.

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

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

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

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

- ✓ Planificació de les feines: Identificació dels centres de la Entitat i, en el seu cas, encarregats del tractament, objecte i 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. 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
	<i>No detectada</i> , és a dir, la situació actual de l'Entitat compleix la normativa.
	<i>Àrea de millora</i> , és a dir, l'estat de la situació actual requereix ésser completat perquè no s'ajustaria íntegrament a l'establert a la normativa.
	<i>Salvetat</i> , és a dir, la situació actual incompleix la normativa i ha de ser modificada de forma prioritària segons les recomanacions efectuades en l'Informe.

4. Dades de l'entitat i treballs efectuats

4.1. Dades identificatives.

4.1.1. Dades de l'entitat

Entitat	COL·LEGI OFICIAL D'INFERMERES I INFERMERS DE BARCELONA
NIF	Q0866003G
Domicili	Carrer Pujades, 350 08019 de Barcelona

4.1.2. Descripció de la 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.

4.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els diversos departaments i serveis de l'entitat:

- ✓ Sistemes d'Informació
- ✓ Àrea de Comptabilitat i Qualitat
- ✓ Recursos Humans
- ✓ Comunicació, acció comercial i màrqueting
- ✓ Atenció al Col·legiat
- ✓ Arxiu i Biblioteca

4.2.1 Data de realització de l'auditoria

Dies	9 i 10 de juliol de 2014
-------------	--------------------------

4.2.2. 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. Albert Tort	President COIB
2	Sr. Joan Conesa	Gerent COIB
3	Sr. Gabriel Bronchales	Responsable Qualitat i Comptabilitat Responsable Fitxer Administració
4	Sra. Conxi Lerma	Administrativa de suport delegacions, màrqueting, borsa de treball Responsable Fitxer Objectores
5	Sra. Sandra Santiago	Administrativa Suport grup 65 Responsable fitxer Voluntaris
6	Sr. , Antonio Torrejón	Director de Sistemes i TICs
7	Sra. Isabel Quintana	Responsable Atenció Col·legial

		Responsable Fitxer Ciutadans
8	Sra. Núria Garcia	Responsable RRHH i Adjunta de Gerència
		Responsable Fitxer Personal
9	Sra. Rosa Rivas	Responsable d'Administració Col·legial
		Responsable Fitxer Col·legiats i No Col·legiats
10	Sra. Maite Framis	Responsable Arxiu i Biblioteca
11	Sr. Jordi Cardila	Suport Arxiu i Biblioteca
12	Sr. Galo Quintanilla	Adjunt Comunicació i Responsable màrqueting

Relació de la documentació lliurada a l'auditor:

Document
Instrucció de Treball - Incidències
Instrucció d Treball - Revisió del sistema
Document de Seguretat
Procediment Fitxer Col·legiats
Procediment Fitxer Administració
Procediment Fitxer Personal
Procediment Fitxer Ciutadans
Procediment Fitxer Voluntaris
Procediment Fitxer Infermeres Objectores
Procediment Fitxer No Col·legiats
Estatuts
Circular informativa
Contractes amb tercers
Informació i compromís del treballador
Codis d'inscripció de fitxers

Manual d'acollida
Mòduls Ulisses
Ulisses: Manual de l'Usuari, Sistema Integral de Gestió
Cartes de Resposta Drets ARCO
Informació i compromís respecte al Deure de Confidencialitat
Compromís de Protecció de dades amb tercers Recerca
Cessió drets d'imatge
Consentiment Informat comunicació dades salut laboral
Consentiment Junta de Govern
Consentiments Infants
Registre d'incidències
Registre Entrada documentació Arxiu general
Registre Exercici drets d'accés, rectificació, cancel·lació i oposició
Registre informe de revisió mensual del sistema
Registre Model d'entrades i sortides.RG03
Registre recepció CV degut a procés de selecció i espontàniament
RG01-PR07-O01 Arxiu Expedient
RG02-PR07-O02 Control Expedients
RG39-PRDades-Entrades i Sortides fitxers
Sortida Documentació Arxiu general.RG18
Evidències auditoria 2014
Acta Comissió Qualitat-Aud.Prot.Dades 12
IT01-PR17-S01-V4.0 Administració d'usuaris
IT02-PR17-S01-V5.0 Seguretat informàtica
IT03-PR17-S01-V3.0 Incidències informàtiques
PR17-S01-V6.0 Manteniment informàtic

- ✓ 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.

5. Anàlisi de les diferents àrees de l'auditoria

I - BLOC GENERAL

5.1. Auditoria.

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

El Col·legi Oficial d'Infermeres i Infermers de Barcelona (COIB) i en endavant l'Entitat, realitzà la darrera auditoria en matèria de protecció de dades al juny de 2012, complint d'aquesta manera amb les previsions de biennalitat establertes per la legislació en protecció de dades.

Les conclusions de l'auditoria anterior van ser analitzades pel Responsable de Seguretat, i posteriorment elevades al Responsable del Fitxer per tal que adoptés les mesures correctores adequades. L'entitat ha fet entrega de l'Acta de Treball, celebrada el 25 de novembre de 2012, on s'exposen els resultats obtinguts i les accions de millora a implementar.

Àrea 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, per a l'exercici de les quals poden utilitzar potestats administratives i altres activitats de naturalesa privada. Per això, els col·legis professionals, poden ser responsables de fitxers de titularitat pública i també de fitxers de titularitat privada.

El fitxer de COL·LEGIATS, en tant que regula les dades de les col·legiades i col·legiats, revesteix naturalesa pública per raó del seu tractament doncs es troba registrat de forma correcta al Registre de Fitxers de Titularitat Pública de l'Autoritat Catalana de Protecció de dades.

Els fitxers ADMINISTRACIÓ, PERSONAL, VOLUNTARIS I INFERMERES OBJECTORES AL RDL 16/2012; es troben registrats a l'Agència Espanyola de Protecció de dades. Els fitxers VOLUNTARIS i CIUTADANS, es troben registrats a l'Autoritat Catalana de Protecció de dades. Tots ells disposen de naturalesa privada.

FITXER	CODI	FINALITAT	NIVELL	TRACTAMENT
Personal	2042100219	La gestió de recursos humans a efectes de selecció de personal, contractació i elaboració de nòmines	Bàsic	Automatitzat
Administració	2042100220	Realització dels processos habituals de facturació, comptabilitat i financers	Bàsic	Automatitzat
Infermeres objectores al RD 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 deixar constància de la seva declaració i als efectes jurídics establerts a l'Ordenament Jurídic	Alt	Mixt
Col·legiats	204200208-K	Gestió de les prestacions col·legials, representació corporativa, ordenació de l'exercici de la professió,	Mig	Parcialment automatitzat

		etc.		
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	Parcialment automatitzat
Fitxer inscripció de no col·legiats	212002264-V	Donar serveis d'assessories, del SBDI, d'esdeveniments, entre d'altres serveis del Col·legi,	Bàsic	Mixt
Ciudadans	214000028-W	Donar opció de consulta i participació al COIB per part dels ciutadans així com atendre queixes i reclamacions	Bàsic	Parcialment automatitzat

Salvetat

▼	Salvetat	Malgrat disposar dels codi d'inscripció, el FITXER D'INSCRIPCIÓ DE NO COL·LEGIATS com el d'INFERMERES OBJECTORES al RD 16/2012, no es troben inscrit al registre de l'APDCAT (consulta registre <i>on-line</i>). El nivell de seguretat del fitxer PERSONAL es troba declarat com BÀSIC; en tant que hauria de ser MIG. Els tractaments dels fitxers ADMINISTRACIÓ i PERSONAL haurien de ser mixt i no automatitzats. Es detecten tractaments de dades no declarats, com per exemple: - La gestió de les dades en referència a la <i>Infermera Virtual</i> - <i>Borsa de treball</i>. Si bé únicament en poden fer ús els col·legiats, la seva finalitat és diferent de la pròpia i estricta del fitxer COL·LEGIADES. O bé, s'amplia la del fitxer existent, o es crea un de nou. Les diferents ASSESSORIES que disposa l'entitat tracten dades molt en particular de les col·legiades/ts i no col·legiades/ts. Pot suposar un tractament de dades de nivell alt; per exemple trobem les Assessories Civil-Penal, Fiscal i Laboral, que molt probablement
---	----------	---

		tractaran dades de nivell mig i alt (Fitxer CIUTADANS).
--	--	---

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 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.
<u>Comentari:</u> • Correcte. L'entitat disposa d'un Document de Seguretat per a cada fitxer registrat (7) davant l'Agència Espanyola de Protecció de Dades o davant l'Autoritat Catalana de Protecció de dades. Malgrat això, hi han annexos i procediments comuns a tots ells.
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.
<u>Comentari:</u> • L'entitat disposa d'inventari de suports amb dades personals. • Es disposa de diagrama de xarxa com les BBDD i programari.
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 (<i>nivell alt</i>).
<u>Comentaris:</u> Les mesures de seguretat (físiques) són les pertinents i necessàries a raó del tractament de les dades.
D. Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigint en el Reglament.
<u>Comentari:</u> L'Entitat disposa de diversos annexes, protocols, procediments i formularis que s'adjunten al document de seguretat.
E. Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers.
<u>Comentari:</u> L'entitat disposa del document <i>Informació i Compromís del treballador</i>, com documentació vers la seguretat de la informació.
F. Procediment de notificació, gestió i resposta davant les incidències.
<u>Comentaris:</u> Correcte. Veure <i>IT03-PR17-S01-V3.0 Incidències informàtiques</i> i <i>l'Annex I - Notificació i Gestió d'incidències</i>, del document de seguretat
G. Procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats.
<u>Comentari:</u> Aquests procediments estan regulats a la pàgina 167 del <i>document de seguretat</i> i a la <i>Instrucció de Treball - Seguretat Informàtica</i>.
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.

<u>Comentaris:</u> • Correcte. Veure pàgina 178 del <i>document de seguretat</i>, i registres.
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.
<u>Comentari:</u> • L'entitat ha de disposar d'un registre amb els tercers encarregats de tractament (veure punt 5.5 del present informe).
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 el document de seguretat oportú la identificació del fitxer o tractament i el seu responsable i les mesures de seguretat a implementar en relació amb el tractament.
<u>Comentari:</u> • No es detecta ni és necessari la citada identificació.
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.
<u>Comentari:</u> • Correcte. Veure punt 8 i 9 del <i>document de seguretat</i>.
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.

<u>Comentari:</u> • L'entitat disposa usuaris/perfils amb accés remot a les BBDD, com terceres empreses.
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.
<u>Comentari:</u> • Correcte. Veure pàgina 165 del <i>document de seguretat</i>, i IT02-PR17-SOI-V5.0 <i>Seguretat informàtica</i>
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.
<u>Comentari:</u> • Correcte. Veure pàgina 73 del <i>document de seguretat</i>.
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.
<u>Comentari:</u> • Correcte. Veure pàgines 76, 78 i 80 del <i>document de seguretat</i>.
P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.
<u>Comentari:</u> • Correcte, veure punts 8 i 9 del <i>document de seguretat</i>.
Q. Personal autoritzat per a la recepció/enviament de dades de caràcter personal (<i>nivell mitjà i/ o alt</i>).
<u>Comentari:</u>

• Correcte. Veure els registres que disposa el COIB el control de l'entrada i sortida, i accés a la documentació.
R. Personal autoritzat per a la realització del procediment de recuperació de dades.
<u>Comentari:</u> • Cal definir el personal autoritzat i procés per a la gestió de la recuperació de dades. Amb tot el procediment es regula al punt 10 del document de seguretat.
S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.
<u>Comentaris:</u> • Correcte. El DS delega funcions com Responsable de Fitxers, i Responsable de tractaments interns.
Altres mesures
T. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat.
<u>Comentaris:</u> • Correcte. Veure pàgina 165 del <i>document de seguretat</i>, i <i>IT02-PR17-SOI-V5.0 Seguretat informàtica</i>.
U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.
<u>Comentari:</u> • Correcte. Veure pàgina 165 del <i>document de seguretat</i>, i <i>IT02-PR17-SOI-V5.0 Seguretat informàtica</i>.
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.

<u>Comentari:</u> A dia d'avui no es té constància no necessitat de la realització de proves per la implantació o modificació dels sistemes d'informació.
W. Identificació del Responsable de Seguretat (<i>nivell mitjà i/ o alt</i>).
<u>Comentari:</u> Correcte.
X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document (<i>nivell mitjà i/ o alt</i>).
<u>Comentari:</u> L'entitat realitza de forma periòdica controls periòdics (veure Annex J del document de seguretat), com les preceptives auditories en compliment dels articles 96 i 110 del RDLOPD.

Àrees de millora

	Àrea de millora	Veure comentaris I i R del quadre anterior. Manca la regulació i descripció de la borsa de treball (seguretat, accessos i <i>hosting</i> de les dades). Els deferents perfils o mòduls de la BBDD <i>ULISSES</i> hauran de fer-se constar al document de seguretat.
---	-----------------	--

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. En el document de seguretat es deixa constància de delegacions cap al Gerent del COIB, com al Responsable de Seguretat i encarregats interns dels fitxers.

Àrees de millora

	No detectada	
---	--------------	--

5.5. Tercers.

ENCARREGATS DE TRACTAMENT

Base legal: Articles 21, 82 i 88.5 del RD 1720/2007, i 12 de la LOPD 15/1999.

Situació actual

El COIB disposa d'un llistat actualitzat amb tercers amb accés a dades; amb la identificació del nom de l'empresa (veure pàgina 81 del document de seguretat):

Un cop realitzat el mostreig dels contractes d'encarregat de tractament, passem a comentar els següents contractes:

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
Softeng S.L.	Gestió i manteniment dels servidors del COIB	✓	Correcte
Kahuna SIT S.L.	Serveis informàtics	✓	Correcte
RSM Advocats	RRHH	✓	Correcte
Contracte Assessor Manel Tomàs	Assessoria en formació i cooperació	✓	Correcte
Contracte Delegats Comarcals	Delegacions comarcals del COIB	✓	Correcte
Plataforma de Organització Logística	Servei mailing	✓	Manca detallar les mesures de seguretat a aplicar per part de l'encarregat de tractament

Àrea de millora

●	Àrea de millora	El COIB amb tot tercer que hi tingui accés a dades (i sota la vessant de l'article 12 de la LOPD), haurà de formalitzar la seva relació amb el model de contracte que empra (exemple amb l'empresa KAHUNA). És necessari llistar els encarregats de tractament, identificant els fitxers o tractaments a tractar en concepte d'encarregat amb referència expressa al contracte o document que reguli les condicions de l'encàrrec, així com la identificació del responsable i del període de vigència de l'encàrrec.
---	-----------------	---

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

Es van analitzar sota la tècnica de mostreig els següents contractes de prestacions sense accés a dades:

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS	COMENTARIS
IF Seven	Neteja		Correcte
Sistemes digitals de Catalunya	Impressores		No es disposa contracte conforme l'article 83 de la LOPD.
Ecològic	Destrucció de paper (sense dades)		Es necessari fer signar la prohibició d'accés a dades com deure de secret, amb tot tercer que no tingui accés a dades.

Salvetat

	Salvetat	Es necessari que l'Entitat faci signar l'acord de prohibició d'accés a dades com compromís de confidencialitat, amb totes aquelles empreses que desenvolupin serveis a les dependències del COIB, i pels quals no hagin d'accedir a dades.
---	----------	--

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 *de cada fitxer* de l'entitat:

TRACTAMENT	LEGITIMACIÓ	COMENTARIS
Personal	Clàusula Addicional Segona del Contracte laboral	Correcte
	Clàusula <i>recepció currículum degut a selecció</i>	Correcte
	Clàusula <i>recepció currículum espontàniament, via correu o en mà</i>	Correcte
	Clàusula Addicional Quarta.- Autorització de l'ús de la imatge	El redactat és correcte, però el treballador hauria de donar el consentiment exprés per l'ús de la seva imatge, i no com un element ja pressupostat del contracte laboral.
Col·legiats	Document d'informació i consentiment per als nous col·legiats	Correcte.

Atenció al ciutadà	El COIB disposa de formulari Web de recollida de dades http://www.coib.cat/QueixesContactUs.aspx?idPagina=1076&mc=9	Les dades formaran part del Fitxer CIUTADANS i no del de COL·LEGIATS. Cal una millor definició de la finalitat de la recollida dades.
	Formulari web biblioteca/suggeriments i consultes http://www.coib.cat/QueixesContactUs.aspx?idPagina=27&idMenu=139	Manca clàusula informativa en referència al tractament de les dades
Voluntariat	Document Compromís - Voluntariat COIB	Manca clàusula informativa en referència al tractament de les dades
Infermeres objectores al RD 16/2012	Revisió del document http://www.coib.cat/uploadsBO/Noticia/Documents/CARTA%20ADHESI%C3%B3%20AL%20REGISTRE%20OBJECTOR.PDF	Manca clàusula informativa en referència al tractament de les dades
Fitxer inscripció no col·legiats	Es revisa el formulari web <i>V Espai de trobada. El temps... El vols veure passar o el vols viure?</i> http://www.coib.cat/esdvForms/frmlInscripcioEsdeveniment.aspx?id=527	Cal una millor definició de la finalitat de la recollida dades, com rectificar al Fitxer de recollida de dades.

Infermera Virtual	Formulari web http://infermeravirtual.com/cat	Manca clàusula informativa en referència al tractament de les dades
Protecció de dades amb tercers. Premis COIB	Es va fer entrega de model document informatiu	Caldria fer menció a que les dades formaran part d'un fitxer titularitat del COIB, i detallar la finalitat de la recollida,
Cessió de drets d'imatge	Document per legitimar l'ús de la imatge en relació a les activitats, cursos...	Fer menció que l'ús que es pot arribar a fer de la imatge (tot i consentiment) no té limitació temporal, no és correcte.
Consentiment junta de Govern	Document d'informació i consentiment per la difusió de la imatge i CV.	El document és correcte, en tant que el COIB legitima i demana l'autorització per la difusió de les dades de la Junta de Govern. Únicament caldria fer menció a que les dades formaran part d'un fitxer titularitat del COIB, la finalitat i l'adreça (física o correu electrònic) per un Dret ARCO.
Consentiment infants	Document per legitimar la difusió de la imatges d'infants	Correcte

Salvetat

	Salvetat	Ampliar els processos de legitimació de dades segons els comentaris del quadre anterior. Recordem que tot formulari de recollida de dades haurà de disposar de clàusula informativa en referència a l'article 5 de la LOPD (ja sigui en paper o suport automatitzat). El COIB disposa de càmeres que s'activen amb sensors de moviment (capturen la imatge), quan les dependències són tancades. Recomanem posar cartells informatius en tant que es disposa de dispositiu de videovigilància. Segons es va posar de manifest, el butlletí electrònic no posa les indicacions de com donar-se de baixa del servei.
---	----------	--

5.7. Drets ARCO.

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

Situació actual

L'entitat disposa de formularis per eventuais drets d'accés, rectificació, cancel·lació i oposició per part dels afectats, com models de resposta. Veure *Annex L* del document de seguretat.

A la pràctica, tot dret ARCO serà exercit davant l'Àrea d'Atenció Col·legial del Col·legi Oficial d'Infermeres i Infermers de Barcelona (on disposen dels formularis model de cada un dels Drets), per escrit i annexant fotocòpia del DNI o document equivalent. Totes elles es registren i es porta un control tant de l'entrada de la petició, com de la sortida. El procediment i circuit establert es troba dissenyat per donar resposta a l'afectat dins del termini establert (veure pàgina 24 a 29 del document de seguretat).

Àrees de millora

	Àrea de millora	El marc legal que disposa els formularis de Drets ARCO -Real Decret 1332/94-, va ser derogat per Real Decret 1720/2007. Cal la seva modificació.
--	-----------------	--

II - BLOC DE MESURES INFORMÀTIQUES

5.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'entitat, al document de seguretat (pàgines 64, 65 i 68), descriu la connectivitat i disposa del diagrama de xarxa; (a les pàgines 62 a 64) descriu la gestió de servidors, bases de dades i entorn operatiu. El COIB disposa de 2 xarxes; la corporativa i una per usuaris externs (convidats) mitjançant WIFI. La seguretat es troba dissenyada mitjançant *firewall* restrictiu de ports i de control d'atacs externs, realitzada pel servidor ISA (COIBISA01), antivirus Eset Endpoint, i antivirus d'actualització diària per als fitxers del propi servidor o qualsevol dispositiu dels clients-usuaris.

L'Entitat disposa d'estacions de treball amb indicacions per a tots els treballadors de no emmagatzemar documents en les memòries internes, doncs habilita ja sigui carpetes de xarxa per als treballadors, com departamentals, si ho creu necessari.

Les principals aplicacions que tracten dades de caràcter personal (es descriuen a cada document de seguretat de forma detallada) , amb tot les principals són les següents:

APLICACIÓ	UTILITAT
Ulisses	Servei d'atenció al Col·legiat
A3 NOM	Gestió de personal
Office	Registres Gestió de dades de voluntariat i objectores
Contaplus (migració al juny/juliol A3 ERP PLUS Integral)	Administració
Microsoft Exchange	Correu electrònic

Àrees de millora

	No detectada	
---	--------------	--

5.9. 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. Com es descriu en el document de seguretat (pàgina 178, punt G7) on consten els accessos a les diferents bases de dades. Diferenciem:

- Junta de Govern
- Gerent
- Direcció de Programes
- Responsables dels diferents Departaments del COIB
- Kahuna (servei informàtic)
- Softeng (servei informàtic)

Tanmateix la xarxa sense fil està desplegada a l'interior de l'edifici, utilitzant tecnologia *IEEE 802.11 abgn*. La xarxa està aïllada físicament dels servidors interns, per als cursos de formació o, en general, per a qualsevol usuari extern que dins les dependències del COIB requereixi de connexió a Internet. Existeixen 7 xarxes sense fils diferents (veure pàgines 66 i 67 del *document de seguretat*).

Àrees de millora

	No detectada	
---	--------------	--

5.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

Les connexions que es van detallar durant els treballs de camp compleixen amb el requeriments de seguretat que estableix el marc normatiu. La descripció de la seguretat per les connexions és a la pàgina 65 del *document de seguretat*; mitjançant *terminal server*, amb requeriment de nom d'usuari i una password.

Àrees de millora

	No detectada	
---	--------------	--

5.11. Control d'accés.

Base legal: Articles 89.I, 91 i RD 1720/2007.

Situació actual

L'entitat disposa d'un procediment al *document de seguretat* on consta l'alta i baixa d'usuaris a les bases de dades que disposa (veure pàgina 162 i següents del *document de seguretat*). El responsable de la creació d'usuaris, així com d'assignar permisos i perfils d'accés, és la Unitat de Sistemes d'Informació, prèvia notificació de Recursos Humans, donant d'alta als recursos necessaris:

- Alta al sistema
- Correu electrònic
- Llistes de distribució
- Carpetes compartides
- Possibilitat de connexió remota
- Impressora
- Mòduls d'accés a Ulisses

Els usuaris només poden accedir a les dades i recursos que necessiten per al desenvolupament de les seves funcions, atès que s'organitzen d'acord amb l'àmbit del lloc de treball i les funcions assignades.

Els mecanismes que impedeixen que els usuaris accedeixin a més dades de les autoritzades és l'ús de contrasenyes. L'Entitat ha facilitat un mostreig del llistat d'usuaris donats d'alta al sistema.

Àrees de millora

	Àrea de millora	Els mòduls (perfils) de la BBDD Ulisses i que es descriuen en el document <u>Ulisses Sistema Integral de Gestió</u> , caldria fer referenciar o citar els perfils en el document de seguretat de l'entitat, com la seva corresponent descripció.
---	-----------------	--

5.12. Identificació i autenticació d'usuaris.

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

Situació actual

L'identificador per a cada treballador és únic, inequívoc i personalitzat de tot l'usuari que vol accedir al sistema d'informació, com de la verificació que està autoritzat. L'entitat disposa d'un *Active Directory* que proporciona la capacitat d'establir un únic inici de sessió i un repositori central d'informació.

En el moment en que es dona d'alta a un usuari, es genera una contrasenya que aquest haurà de modificar de manera obligatòria en el primer accés al sistema.

La nova contrasenya escollida per l'usuari haurà de contenir un mínim de 6 dígit, ha de contenir 3 d'aquestes categories: majúscules, minúscules, números i símbols. El sistema obliga al seu canvi cada 3 mesos i es guarda de forma intel·ligible.

El número d'intents o possibles errades a l'hora d'introduir la contrasenya serà d'un màxim de 3 consecutius. Arribat aquest número d'intents el compte quedarà blocat fins que un administrador el restableixi o fins que el temps de bloqueig s'esgoti (30 minuts).

En el cas que un usuari deixi el seu ordinador inactiu, aquest es bloquejarà passats 10 minuts. La represa del treball implicarà la desactivació de la pantalla protectora amb la introducció de la contrasenya corresponent.

L'entitat descriu satisfactòriament la gestió de la política de seguretat de les paraules de pas en el *document de seguretat*, pàgina 165.

Àrees de millora

	No detectada	
---	--------------	--

5.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

La mesura de seguretat referent al control dels accessos a les BBDD del COIB no és d'aplicació, en tant que l'entitat no gestiona cap base de dades de nivell alt en suport automatitzat.

Àrees de millora

	No detectada	
---	--------------	--

5.14. Còpies de seguretat.

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

Situació actual

La descripció del procediment de còpies de seguretat resideix al document de seguretat (pàgina 167), i en el document *Instrucció de Treball - Seguretat Informàtica*. El procediment resideix en:

- Diàriament es realitza una còpia de seguretat a cinta.
- Setmanalment es realitzarà un còpia en cinta amb les mateixes dades que el backup diari.
Les còpies setmanals seran custodiades pel COIB en la seva mateixa seu social en una caixa forta.
- Mensualment es realitzarà un còpia en cinta amb les mateixes dades que el backup diari.
La darrera còpia mensual serà custodiada pel COIB fora de la seva seu social per tal de garantir el control dels registres derivats de la seva pròpia activitat (caixa forta d'entitat bancària).
- Anualment es realitzarà una còpia en cinta amb les mateixes dades que el backup diari.

L'entitat ha designat al Responsable de Qualitat, com a autoritzat per traslladar les cintes de seguretat del COIB al banc, i es disposa de registre, com totes elles van correctament etiquetades .

El procediment de recuperació i restauració de dades es regula en el punt 10 del *document de seguretat*.

Tots dos processos, garanteixen en tot moment la reconstrucció en l'estat en que es trobaven les dades al produir-se la pèrdua o destrucció.

L'entitat va fer entrega del registre de comprovacions de backup.

Àrees de millora

	No detectada	
---	--------------	--

5.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

En primer lloc, destacar que l'existència de fitxers temporals ofimàtics és inherent al funcionament de qualsevol entitat que disposi de Microsoft Office. És habitual la utilització documents office per a la gestió de registres, voluntariat i objectores; però no suposa una duplicitat de les BBDD ni fitxers temporals, és més, el document de seguretat ho prohibeix de forma expressa.

Àrees de millora

	No detectada	
---	--------------	--

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

Base legal: Article 97 RD 1720/ 2007.

Situació actual

L'entitat regula la gestió d'entrades i sortides de suports automatitzats als punts 8 i 9 del document de seguretat.

“Totes les entrades i sortides de dades dels Fitxers que s'efectuïn mitjançant correu electrònic es realitzaran des del compte o adreça de correu de l'usuari o usuaris especialment autoritzats pel responsable del Fitxer i detallat en l'Annex F. Igualment si es realitza l'entrada o sortida de dades mitjançant sistemes de transferència de fitxers per xarxa, únicament un usuari o administrador estarà autoritzat per realitzar aquestes operacions.

Es guardaran còpies de tots els correus electrònics que involucrin entrades o sortides de dades dels Fitxers, en directoris protegits i sota el control dels responsable. També es guardaran en directoris protegits, una còpia dels fitxers rebuts o transmesos per sistemes de transferència de fitxers per xarxa, juntament amb un registre de la data i hora en què es va realitzar l'operació i la destinació o l'origen del fitxer rebut o enviat.”

Àrees de millora

	No detectada	
---	--------------	--

III- BLOC DE MESURES FÍSQUES 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

L'entitat disposa d'un inventari i registre de tots els suports, i tots ells degudament identificats.

La gestió dels suports informàtics (manteniment i destrucció) és gestionada per un tercer, *Kahuna*.

L'entitat disposa de destructores de paper a diferents àrees de treball. Es descriu la gestió de la documentació com dels suports, a la pàgina 178 del document de seguretat.

En relació als dispositius d'emmagatzematge externs (possibles portàtils, *smartphones*...), la seva gestió i treball és segura i sense necessitat de xifratge del disc dur. Tanmateix es disposa d'un control sobre tots ells. Citem el DS, pàgina 178, sobre el seu ús:

“Només els membres de la Junta de Govern, Gerent, Direcció de Programes i resta de Responsables dels diferents Departaments del COIB tenen dret a l'ús dels portàtils amb connexió remota i a la configuració del correu electrònic als dispositius mòbils”.

Àrea de millora

	No detectada	
---	--------------	--

5.18. Control d'accés.

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

Situació actual

Els arxius que disposen de dades de caràcter personal disposen de mecanismes de tancament, i únicament hi té accés el personal autoritzat, veure pàgina 80 del *document de seguretat*.

La descripció dels arxius i personal autoritzat és la següent:

- Armari amb dades del personal. Situat a l'àrea de Gerència. Disposa de la clau el Gerent
- Armari amb dades d'administració. Ubicat a Comptabilitat. Disposa de la clau el Comptable
- Armari amb dades de les infermeres objectores. Ubicat a Gerència. Disposa de la clau la Responsable de tractament d'aquest fitxer.
- Armari amb dades de Voluntaris. Ubicat a Direcció de Programes. Disposa de la clau la Responsable de tractament d'aquest fitxer.
- Control d'accessos a la sala d'expedients (veure pàgina 76 del DS).
- Control d'accessos a l'arxiu general (veure pàgina 78 del DS).

En relació a la sala del CPD i serveis d'informació, només hi pot accedir el personal autoritzat al DS (veure pàgina 73): Administrativa de referència, Responsable del suport informàtic, el Responsable de manteniment, l'Adjunta a Gerència, el Director de Sistemes i TICs.

Àrees de millora

	No detectada	
---	--------------	--

5.19. Registre d'accessos.

Base legal: Article 113 RD 1720/2007.

Situació actual

Recordem que l'article 113.2 del RD 1720/2007 disposa “S’han d’establir mecanismes que permetin identificar els accessos realitzats en el cas de documents que puguin ser utilitzats per múltiples usuaris”. L'accés a la documentació és únicament pel personal autoritzat, i en el supòsit del *Fitxer Objectores* es disposa de mecanismes on poder fer la correcta traçabilitat de les dades en supòsits d'accés per múltiples usuaris (registre en full *Excel*).

Finalment comentar que l'entitat porta un registre d'accessos a l'arxiu col·legial (expedients), com a l'arxiu documental.

No detectada

	No detectada	
---	--------------	--

5.20. Criteris d'arxiu.

Base legal: Articles 106 RD 1720/2007.

Situació actual

Tot seguit es fa un anàlisi dels criteris d'arxiu, d'acord amb les revisions efectuades i descrites durant els treballs de camp:

Col·legiats:

L'entitat disposa al *document de seguretat* del Fitxer Col·legiats, on descriu de forma detallada l'arxiu de la documentació referent als expedients dels Col·legiats del COIB.

Els expedients resideixen a la planta baixa de l'entitat, en un arxiu amb registre d'accessos i endreçat per ordre numèric de col·legiat.

Recursos Humans

L'arxiu està ubicat al despatx de Gerència, en armaris tancats, i endreçats per números (es disposa d'un llistat amb la preceptiva correlació).

Voluntaris

El COIB disposa d'un portafoli amb cada un dels voluntaris (entre 20-30) a l'Àrea de Direcció de Programes.

Administració

La documentació generada per l'Àrea d'Administració es divideix sota tres criteris d'arxiu:

- Exercici de l'any comptable
- Exercici anterior
- Arxiu general

Objectores

Les declaracions segons el Reial Decret Llei 16/2012, de 20 d'abril, i el Reial Decret 1192/2012, de 3 d'agost; es troben en una carpeta i sota custòdia de la seva responsable.

L'arxiu de tota la documentació es realitza seguint uns criteris adequats i oportuns, que permeten la correcta conservació dels documents, la seva localització, consulta i la possibilitat d'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

L'entitat disposa d'un control de les entrades i sortides, com es corrobora en el document de seguretat *Annex G - 5*.

Les principals sortides (regulars i periòdiques), són:

- Còpies de seguretat, externalitzat cap a entitat bancària.
- Tramesa mensual de nòmines.
- Trasllet d'expedients.
- Sortida de dades a l'estranger.

Àrees de millora

	No detectada	
---	--------------	--

5.22. Fitxers temporals.

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

Situació actual

L'entitat disposa de mecanismes de destrucció de paper. Al *document de seguretat* (veure pàgina 184) s'estableixen les directrius per a l'eliminació dels fitxer temporals una vegada deixin de ser necessaris per als fins que van motivar la seva creació. Es va percebre una bona *praxi* i compliment de la mesura de seguretat.

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

L'entitat disposa del document *Instrucció de Treball - Incidències informàtiques*, com l'*Annex I - Notificació i Gestió d'incidències*, del document de seguretat.

Quan un treballador detecta una incidència que afecti a la seguretat de les dades personals, ho comunicarà i registrarà mitjançant el *model registre d'incidències*, el farà arribar a l'encarregat del tractament del fitxer intern, que decidirà entorn a la seva gestió i resolució. Determinada i registrada la incidència, ho posarà en coneixement del Responsable del Fitxer i del Responsable de Seguretat, informant de les mesures adoptades i resultat de les mateixes.

El Responsable de Seguretat s'encarregarà de relacionar totes les incidències dels diversos fitxers en un document anomenat *Llistat d'incidències*.

Àrees de millora

	No detectada	
---	--------------	--

5.24. Difusió de funcions i obligacions.

Base legal: Article 89.2 RD 1720/2007.

Situació actual

Tot treballador de l'entitat signa el document *Informació i Compromís del Treballador*, a raó del secret professional per les dades a que tingui coneixement.

El treballador disposa al mateix document de les polítiques generals del COIB per preservar la confidencialitat de les dades.

Finalment indicar que l'entitat preveu la possibilitat de sanció cap al treballador, en supòsits d'infraccions de les polítiques establertes en el marc de la protecció de dades (veure Clàusula Addicional Sisena del contracte laboral).

Àrea de millora

	No detectada	<i>Recomanem la realització de sessions de formació de forma periòdica vers la protecció de dades, seguretat de la informació i bones pràctiques; vers al tractament de dades de caràcter personal.</i>
---	--------------	---

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:

AREES DE MILLORA
I- BLOC GENERAL
5.3. Document de seguretat
5.5.. Tercers. Encarregats de tractament
5.7. Drets ARCO
II- BLOC MESURES INFORMÀTIQUES
5.11. Control d'accés

SALVETATS
I- BLOC GENERAL
5.2. Aspectes generals
5.5. Tercers. Prestacions sense accés a dades
5.6. Legitimació de dades

Barcelona, 31 de juliol de 2014.

Pere Ruiz Espinós

- Soci -