ASSOCIACIÓ DE LA PARÀLISI CEREBRAL - ASPACE

INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Número de Protocol 10.320

ÍNDEX

1. Objectius i contingut

De conformitat amb el que estableix la normativa vigent sobre protecció de dades[1], tots els responsables de fitxer i/o encarregats de tractament que disposin de fitxers automatitzats i no automatitzats que continguin dades de nivell mitjà i/o alt, hauran de sotmetre, de forma biennal, els seus sistemes d'informació i instal·lacions de tractament de dades a una auditoria.

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

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

Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (publicat en el BOE número 17, de 19 de gener de 2008).

Codi tipus de la Unió Catalana d'Hospitals.

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	Associació de la Paràlisi Cerebral (ASPACE)
NIF	G08393936
Domicili	Carrer Tres Pins Núm. 29 – Parc de Montjuïc (Centre Pilot) 08038, Barcelona

3.1.2. Descripció de l'activitat

L'Associació de la Paràlisi Cerebral és una organització declarada d'utilitat pública que té com a finalitat l'atenció i la protecció, integració i rehabilitació integral d'aquelles persones i familiars afectats amb paràlisi cerebral i patologies afins mitjançant la realització de tot tipus d'activitats mèdiques, culturals, esportives i de qualsevol altre àmbit.

Amb aquestes finalitats, l'Entitat manté oberts els següents serveis:

- *Escola d'educació especial*: on s'atenen aquells usuaris afectats per paràlisi cerebral i patologies afins d'entre 3 i 21 anys.

- *Centre Pilot Arcàngel Sant Gabriel*: on es presten els serveis d'atenció ambulatòria, hospitalització parcial, rehabilitació, diagnòstic, tractament precoç, teràpia psicològica individual i familiar i exploracions complementàries. (audiometries, electroencefalogrames, proves d'oftalmologia, toxina botulínica, entre d'altres).

- *Residència*: on s'ofereixen els serveis d'acolliment residencial amb caràcter permanent substitutori de la llar i d'assistència integral a les activitats bàsiques de la vida diària per a persones amb paràlisi cerebral que precisen del suport generalitzat degut a problemes de salut.

- *CDIAP*: Centre de Desenvolupament Infantil i Atenció Precoç per a nens i nenes que presenten trastorns de desenvolupament d'entre 0 a 6 anys situat al districte de Sants-Montjuic.

- *Centre d'Integració Social ASPACE Badalona*: que atén a persones adultes amb paràlisi cerebral i patologies vinculades proporcionant-los serveis de teràpia ocupacional i ajustament personal.

- *Centre de Teràpia Ocupacional-ASPACE Poblenou*: que atén a persones amb paràlisi cerebral i patologies afins severes, proporcionant-los serveis de teràpia ocupacional i d'ajustament personal.

- *Centre de Recursos i Tecnologies de Suport (CRA):* on s'atenen a pacients afectats amb aquestes patologies per tal de promoure la seva autonomia personal i integració social.

- *Serveis d'Oci i Esports:* orientats a l'ocupació del temps de lleure i a la rehabilitació mitjançant l'esport.

- *Serveis de Respir i Lleure*: orientats a l'ocupació del temps lliure.

3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els diversos serveis i àrees del centre:

- Centre Pilot Arcàngel Sant Gabriel:
    - Àrea de Sistemes d'Informació i TIC.
    - Àrea de Recursos Humans.
    - Àrea d'Administració.
    - Àrea Mèdica.
    - Àrea de Docència.
    - Àrea de Recerca.
    - Àrea de Comunicació.
    - Àrea d'Arxiu.
    - Àrea d'ASPACE Llar i Oci.

- Centre de Teràpia Ocupacional del Poble Nou:
    - Àrea de Direcció.
    - Àrea d'Arxiu.

- Centre d'Integració Social de Badalona:
    - Àrea de Direcció.
    - Àrea d'Arxiu.

Cal tenir en compte que durant el desenvolupament dels treballs de camp no van poder verificar-se les instal·lacions del Centre de Recursos Tècnics (CRA). En aquest sentit, els apunts es fonamenten a l'afirmació de l'Entitat de que la delegació afectada no ha patit canvis des de la darrera auditoria i es gestiona amb una metodologia equivalent a la que apliquen la resta de centres.

Pel que fa a espais físics, a més de les indicades àrees, s'han revisat els arxius, els despatxos i la sala de servidors del Centre Pilot.

3.2.1. Data de realització de l'auditoria

Dia	27 i 28 de març de 2017

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	Sra. Yolanda Elipe	Responsable de Seguretat
2	Sr. Paul Mussach Rodríguez	Responsable de Seguretat i d'Informàtica
3	Sra. Marta Borràs	Directora de RRHH i Salut Laboral
4	Sres. Mònica Sala i Anna Martínez	Equip directiu de l'Escola d'Educació Especial
5	Dra. Anna Fornós	Direcció Assistencial
6	Sra. Laura Panadero	Treballadora Social
7	Sr. José María Aguilar	Cap d'Admissions i Programació
8	Sr. Albert Cantó	Responsable d'Administració
9	Sra. Míriam Torrella	Directora de Serveis Comunitaris i responsable de Comunicació
10	Sra. Bianca Palmisano	Responsable de Lleure i Respir
11	Sr. Josep Mauri	Direcció del Centre de Teràpia Ocupacional del Poble Nou
12	Sra. Marina López	Direcció del Centre d'Integració Social de Badalona

Relació de la documentació lliurada a l'auditor:

Document
Estatuts
Organigrama
Cartes de l'Agència Espanyola de Protecció de Dades amb els codis d'inscripció dels fitxers
Documents de Seguretat
Mapa de xarxa

Manual i Decàleg de Bones Pràctiques
Fulls d'informació i consentiment, autoritzacions i formularis per a la legitimació de dades
Clàusules, contractes, convenis i acords amb tercers
Mostreig de registres d'entrades i sortides
Registre d'accessos i d'incidències
Formularis Drets ARCO

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

D'acord amb l'article 96 RLOPD, a partir del nivell mitjà, els sistemes d'informació i les instal·lacions de tractament i emmagatzematge s'han de sotmetre, amb caràcter mínim biennal, a una auditoria que verifiqui el compliment de la LOPD. En aquest sentit, l'Entitat ha fet entrega de la darrera auditoria, la qual va ser emesa a data de 15 d'abril del 2015, donant amb això compliment a la previsió esmentada.

Addicionalment, el punt tercer del mateix precepte estableix que l'informe resultant de l'auditoria haurà de ser analitzat pel Responsable de Seguretat, que elevarà les conclusions al Responsable del Fitxer per tal de que procedeixi a adoptar les mesures correctores adients, les quals quedaran a disposició de l'Agència Espanyola de Protecció de Dades.

En aquest sentit, ASPACE ha lliurat l'Acta per la qual s'elevaren els resultats de l'informe d'auditoria, la qual va ser emesa el 14 de gener del 2016.

Àrea de millora

▲	No detectada	

5.2. Aspectes generals.

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

Situació actual

De la documentació aportada i de les consultes formulades al Registre de l'Agència Espanyola de Protecció de Dades (en endavant, AEPD) consta, que a data de la present Auditoria, l'Entitat té enregistrats els següents fitxers:

FITXER	CODI	FINALITAT	NIVELL	TRACTAMENT
Dades pacients	2030510121	Gestió de les visites.	Alt	Parcialment Automatitzat
Administració ASPACE Barcelona	2031330129	Gestió administrativa de l'Entitat.	Mitjà	Parcialment Automatitzat
Comunicació i Socis	2130160218	Gestió de socis i comunicació.	Bàsic	Automatitzat
Recursos Humans	2031320090	Gestió de personal.	Alt	Automatitzat
Investigació Clínica	2141920701	Realització i seguiment de la investigació clínica de l'Entitat.	Alt	Automatitzat
Videovigilància	2141272544	Videovigilància i seguretat dels accessos i de l'interior de les instal·lacions.	Bàsic	Automatitzat

Àrees de millora

▲	No detectada	*En tant que entitat subjecta a la Llei 10/2010 de Prevenció de blanqueig de capitals i del finançament del terrorisme (LBPC), segons l'article 2.1.x); respecte a la recepció i a l'atorgament de donacions, es preveu l'aplicació de mesures d'identificació en relació a les quals caldrà notificar la creació del Fitxer de Prevenció de Blanqueig de Capitals, d'acord amb l'article 32 de la LPBC.*

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 DS per a cadascun dels fitxers que té declarats davant l'AEPD, l'última versió dels quals data de març del 2015. • Malgrat això, els DS lliurats no han estat signats per part de la Direcció General, com a prova de la seva aprovació i coneixement.
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: • La ubicació del llistat amb l'inventari consta referenciada com a document annex del DS; al *Reg 01-Registre de Repositoris Físics.* • Correcte. La informació relativa a l'estructura dels fitxers es descriu al punt 2 de cadascun dels DS que corresponen als fitxers declarats.
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: • És correcte. No consta que s'hagin d'aplicar mesures alternatives.
D. Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit en el Reglament.
Comentaris: • Correcte. El DS es nodreix d'un seguit d'annexes on es desenvolupen les normes, procediments, regles i estàndards encaminats a garantir el nivell de seguretat que enuncia la normativa legal vigent en matèria de protecció de dades.
E. Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers.
Comentaris: • L'Entitat disposa de la Guia de Bones Pràctiques i d'un Decàleg d'Actuacions on recorda als professionals determinades actuacions que es consideren com a prohibides. Igualment, a cadascun dels DS de l'Entitat s'inclou una referència a la Política de Seguretat, on s'hi desenvolupen extensament les funcions i obligacions del personal.
F. Procediment de notificació, gestió i resposta davant les incidències.
Comentaris: • És correcte. El procediment de notificació i tramitació tant de les incidències de seguretat informàtiques, com de les incidències no informàtiques es descriuen al punt 5 de la Política de Seguretat de la Informació i en el seu Annex 14- *Gestió d'incidències.*
G. Procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats.

Comentaris:

- És correcte. Es regulen als punts 4.3.8 i 4.3.9 de la Política de Seguretat de la Informació.

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:

- Les mesures relatives a la destrucció i reutilització de suports i documents, es detallen al punt 4.3.11 de la Política de Seguretat de la Informació i, paral·lelament, en el seu *Annex 9- Procediment de destrucció i esborrat.*

- Les especificacions relatives al transport de documentació i suport físic consten al punt 4.2.6 de la Política de Seguretat de la Informació.

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

Comentari:

- L'Entitat disposa d'un llistat d'encarregats de tractament on s'hi conté la relació dels contractes atorgats. De la mateixa manera, els DS fan una menció als encarregats de tractament en la Política de Seguretat de la Informació i també en l'Annex 10.

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:

- L'Entitat no disposa d'un llistat on hi enregistri els serveis que els hi presta com a Encarregat de Tractament a terceres entitats (Institut ASPACE Fundació Privada).

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.
Comentaris: • Correcte. Es regula al punt 4.2.4 de la Política de Seguretat de la Informació.
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: • S'hi estipulen als punts 4.2.7 i 4.3.2 de la Política de Seguretat de la Informació i al Reg 07- Llistat d'autoritzacions per a accés remot que s'acompanya com a document annex de la mateixa.
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: • Es regula al punt 4.4 de la Política de Seguretat de la Informació i en els punts 5.1 dels DS.
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: • Trobem aquesta referencia en el Reg 01- Registre de repositoris.

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: • Aquest aspecte es regula al punt 3.5.1 del Ds d'investigació clínica, al 5.3 dels de pacients, recursos humans i administració i en el 5.2 del DS de comunicació.
P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.
Comentari: • És necessari descriure les vies i persones autoritzades per a la sortida d'informació amb dades personals, incloent els autoritzats per emprar l'eina del correu electrònic per aquesta tasca.
Q. Personal autoritzat per a la recepció/ enviament de dades de caràcter personal *(nivell mitjà i/ o alt).*
Comentari: • És necessari descriure les vies i persones autoritzades per a la recepció així com enviament de dades personals pel que fa a les dades de nivell mitjà i/o alt.
R. Personal autoritzat per a la realització del procediment de recuperació de dades.
Comentari: • Cap dels DS fan referència al procediment de recuperació de dades, així com tampoc al personal autoritzar a portar-lo a terme en cas de necessitat.. Respecte a aquest procés, només s'hi fa una petita referència en el punt 4.3.8 de la Política de Seguretat de la Informació.
S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.

Comentari: • No sempre es referencia la persona sobre la qual recauen les esmentades autoritzacions.
Altres mesures
T. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat.
Comentaris: • Es regulen en el punt 4.4.3 i en l'Annex 3 de la Política de Seguretat de la Informació.
U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.
Comentari: • S'hi preveu en l'Annex 3 de la Política de Seguretat de la Informació.
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: • Consta en el punt 4.4.6 de la Política de Seguretat de la Informació.
W. Identificació del responsable de seguretat *(nivell mitjà i/ o alt).*
Comentari: • Consten al punt 9.4 de la Política de Seguretat de la Informació.

X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt)*.
Comentari: • Es descriu en el punt 6 de la Política de Seguretat de la Informació.

Àrees de millora

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

5.4. Delegació d'autoritzacions.

Base legal: Article 84 RD 1720/2007.

Situació actual

L'article 84 del RLOPD estableix la possibilitat de delegar en d'altres persones les responsabilitats atribuïdes al Responsable del Fitxer. Aquells qui hagin estat habilitats per a l'atorgament de les autoritzacions i els qui siguin nomenats per al desenvolupament de les esmentades tasques hauran de romandre identificats al Document de Seguretat sense que, en cap cas, es pugui entendre que aquesta delegació podrà suposar la descàrrega de les responsabilitats que li són inherents al Responsable del Tractament.

Arrel de l'observació de la documentació lliurada, al punt 9.4 de la Política de Seguretat de la Informació s'estableix la delegació de determinades funcions cap als Responsables de Seguretat nomenats a l'efecte.

Addicionalment, al llarg del document s'inclouen diverses referències a d'altres persones a les que els hi han estat atribuïdes d'altres delegacions.

Àrea de millora

▲	No detectada	

5.5. Tercers.

ENCARREGATS DE TRACTAMENT

Base legal: Article 82 RD 1720/2007.

Situació actual

L'Entitat ha posat a l'abast alguns dels contractes concertats amb els diferents prestadors vers als que s'ha realitzat el següent mostreig:

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
SICSA	Servei de manteniment i gestió de software	☑	És correcte segons les especificacions de l'article 12 de la LOPD.
ASPACET	Serveis de destrucció de documentació confidencial, disseny gràfic, impressió digital, gestió web i XXSS, mailings i tractament de BBDD	☑	És correcte segons les especificacions de l'article 12 de la LOPD.
MDA ARCHIVOS	Servei de custòdia de les històries clíniques en paper	☑	És correcte segons les especificacions de l'article 12 de la LOPD.
SANED	Servei de cuina	☑	És correcte segons les especificacions de l'article 12 de la LOPD.
CONFEDERACION ASPACE	Podologia	☑	És correcte segons les especificacions de l'article 12 de la LOPD.
ORTOPEDIA SOM	Serveis d'ortopèdia	☑	És correcte segons les especificacions de l'article 12 de la LOPD.
RAVIGO	Servei de transport d'usuaris d'escola / CTO's	☑	És correcte segons les especificacions de l'article 12 de la LOPD.

Àrea de millora

▲	No detectada	

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

S'han revisat els següents contractes amb tercers sense accés a dades:

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS	COMENTARIS
PLIS-PLAS	Neteja de vidres	☑	El compromís de confidencialitat és correcte en els termes exigits per l'art. 83 del RLOPD.
BLANCH	Manteniment d'aire condicionat	☑	El compromís de confidencialitat és correcte en els termes exigits per l'art. 83 del RLOPD.
MULLOR	Neteja	☑	El compromís de confidencialitat és correcte en els termes exigits per l'art. 83 del RLOPD.
SISTEMES DE CATALUNYA	Manteniment de màquines de reprografia i copiadores	☑	El compromís de confidencialitat és correcte en els termes exigits per l'art. 83 del RLOPD.

Àrees de millora

▲	No detectada	

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
Pacients	Rètols informatius instal·lats a les àrees de recepció i admissió dels pacients.	Correcte, inclou la clàusula de l'article 5 de la LOPD.
	Full de legitimació de dades	El document inclou la clàusula informativa de l'art. 5 de la LOPD. Tanmateix, s'haurà de modificar el model atès que s'hi preveu que el responsable del fitxer és la direcció mèdica del centre quan realment ho és la pròpia Entitat. D'altra banda, en el moment en que l'Entitat incorpori la cessió de dades a l'HC3, caldrà incloure el redactat següent en el Full de legitimació: "*El centre posa en el seu coneixement que participa en la Història Clínica Compartida de Catalunya. Les dades dels pacients als que es presti assistència en aquest centre quedaran integrades en la Història Clínica Compartida de Catalunya, d'acord amb els requeriments legals i seguint les indicacions del Departament de Salut de la Generalitat de Catalunya, que és el responsable d'aquest fitxer. Si desitja rebre major informació o vol exercir els seus drets d'accés, rectificació, oposició o cancel·lació reconeguts en la normativa de protecció de dades, podeu contactar amb _____ del centre".*

	Formularis del servei de Lleure i Respir	Les clàusules informatives que incorporen les autoritzacions per a les sortides i activitats organitzades pel servei preveuen que les dades seran contingudes al fitxer de RRHH, essent la denominació correcta la del fitxer de Pacients. Igualment, alguns dels formularis lliurats a les famílies per tal de que autoritzin les sortides dels usuaris no inclouen el dret d'informació de l'art. 5 de la LOPD.
	Contracte de prestació de serveis assistencial de la Residència d'ASPACE Montjuïc	El contracte incorpora la clàusula informativa de l'article 5 de la LOPD. Si més no, cal incorporar la denominació del fitxer al que s'inclouran les dades.
	Fulls d'autorització per a la presa d'imatges de l'alumne, Fulls d'autorització de sortides i Fulls d'autorització per a dur a terme activitats esportives de l'Escola d'Educació Especial	Els formularis inclouen la clàusula informativa de l'art. 5 de la LOPD, tot i així falta incloure la denominació del fitxer al que s'inclouran les dades.
Comunicació i Socis	Autorització per a la publicació d'imatges a les xarxes socials	Correcte, inclou la clàusula de l'article 5 de la LOPD.
Recursos Humans	Informació i compromís de l'empleat	El document incorpora la clàusula informativa de l'art. 5 de la LOPD. Si més no, no s'inclou l'adreça davant de la que es podran exercir els drets ARCO i s'identifica el responsable del fitxer amb el responsable de RRHH quan realment ho és l'Entitat.
	Informació enviada al correu electrònic en l'entrega de Curriculums Vitae.	La clàusula de resposta automàtica remesa per a la recepció dels cv es suficient en els termes requerits per la normativa.
	Negativa per part del treballador a l'examen de salut de caràcter voluntari	El formulari no inclou la clàusula informativa de l'article 5 de la LOPD.

	Full d'Informació i compromís, Formulari de dades personals i Full de cessió dels drets d'imatge de voluntaris	Correcte, inclou la clàusula de l'article 5 de la LOPD.
Investigació Clínica	Consentiments Informats	Tot i que el model de consentiment informat lliurat als pacients per a la participació en estudis de recerca incorpora la clàusula informativa de l'art. 5 de la LOPD, aquesta no inclou la denominació del fitxer on s'inclouran les dades, ni l'adreça del responsable on podran exercitar els drets ARCO.
Videovigilància	Rètols informatius per a la presa d'imatges.	La informació continguda en els cartells és suficient en els termes requerits per la norma.

Àrea de millora

●	Àrea de millora	Veure els comentaris del quadre anterior.

5.7. Drets ARCO.

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

Situació actual

L'apartat 8 de la Política de Seguretat de la Informació s'ocupa de la gestió dels drets dels usuaris i de la regulació de l'exercici dels drets ARCO. Addicionalment, s'hi preveuen els aspectes a considerar davant la presentació de possibles queixes. De la mateixa manera, als DS de cadascun dels fitxers de què disposa l'Entitat, s'hi inclou una remissió expressa vers a aquest punt en relació al desenvolupament del procediment.

Per mitjà de l'Annex 5 del protocol, s'hi acompanyen a més els formularis tipus a través dels que es podran vehicular les sol·licituds per part dels interessats.

Tot i que a efectes de la tramitació interna del circuit, els escrits haurien de dirigir-se en primer terme al Cap d'Admissions del Centre Pilot, l'Entitat informà que a la data de realització dels treballs de camp encara no s'havien rebut mai peticions d'aquest tipus.

Àrea de millora

▲	No detectada	

II - BLOC DE MESURES INFORMÀTIQUES

5.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'arquitectura del sistema es troba generalment definida en el document d'Auditoria TIC v. 4, tot i que també hi trobem referències a alguns dels seus aspectes a diversos punts de la Política de Seguretat de la Informació.

Pel que fa al mapa de xarxa, durant els treballs de camp apuntaren que cadascun dels centres de l'Entitat disposa del seu propi servidor, tot i que el CPD principal s'ubica a les instal·lacions del Centre Pilot, que es replica contínuament amb el de la Residència i que es connecta per MPLS amb els de la resta. Si més no, actualment ASPACE encara està treballant en el procés d'integració d'una xarxa centralitzada i d'unificació dels dominis.

Tota l'estructura està dotada d'un Firewall integrat al router d'ONO, el qual fa el filtratge de les comunicacions. A més, els dispositius tenen instal·lat l'antivirus Avira.

Les aplicacions detectades durant el treball de camp emprades per l'Entitat són:

APLICACIÓ	UTILITAT
SOCIAL SIC	Gestió assistencial d'usuaris, Escola, Residència i Centres Ocupacionals
A3	Gestió de nòmines
ZKTIME	Control de Presència
VISITES	Control i programació de visites
SIRE	Sistema de recepta electrònica
OFFICE 365	Web i correu electrònic

Àrees de millora

▲	No detectada	

5.9. Connexions remotes.

Base legal: Article 86 RD 1720/2007.

Situació actual

La Política de Seguretat de la Informació tracta aquesta matèria en el seu punt 4.3.4.

Donat que per la tipologia d'activitats que realitzen resulta necessari que alguns dels professionals del centre es connectin des de fóra de l'Entitat, aquesta ha previst la possibilitat d'establir connexions remotes a través d'una VPN.

Concretament, fan ús d'aquesta eina tant el personal que integra el Departament de Sistemes d'Informació, com els responsables de lleure i de la Residència o algun proveïdor extern. Aquestes autoritzacions han quedat enregistrades en el Reg 07- Llistat d'autoritzacions per a accés remot, que s'incorpora dins de l'Annex I de la Política de Seguretat de la Informació.

Àrea de millora

▲	No detectada	

5.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

El punt 4.2.7 de la Política de Seguretat de la Informació determina que caldrà encriptar aquelles dades de nivell alt que s'enviïn per mitjans telemàtics de forma que s'impossibiliti l'accés a la informació per part de tercers no autoritzats. Igualment, el procediment per dur a terme l'obligació de xifratge, es descriu en l'Annex 2 de la Política de Seguretat de la Informació; que el complementa.

Addicionalment, tant a la Guia de Bones Pràctiques, com al Decàleg de Protecció de Dades, s'hi estableixen indicacions al respecte.

En aquest sentit, cal esmentar que durant els treballs de camp s'informà que tots els usuaris que disposen de correu electrònic corporatiu gaudeixen de la possibilitat d'annexar documents i que, a nivell d'Aspace s'empren uns sistemes de xifratge que ofereixen una encriptació de la qualitat (AES-256), atenent amb això al compliment dels requisits establerts per l'Agència de Protecció de Dades en matèria de seguretat mínima.

D'altra banda, és necessari apuntar que pel que fa a l'ús del fax aquest es troba totalment prohibit per a l'enviament de dades personals de nivell alt.

Àrees de millora

▲	No detectada	

5.11. Control d'accés.

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

Situació actual

Al punt 4.4.1, com al 4.4.4 de la Política de Seguretat de la Informació es determina que les funcions i obligacions dels usuaris per a accedir a les dades vindran definides en funció del rol i la categoria professional que desenvolupa en el si de l'Entitat. En aquest sentit, en l'Annex 10 de l'anterior protocol, és on s'ha establert el llistat amb els perfils dels empleats i els permisos que els hi han estat associats als aplicatius amb els que treballen.

Tanmateix, durant la realització dels treballs de camp s'informà que els procediments d'alta i baixa dels usuaris es gestionen per part del Departament de Sistemes. D'aquesta manera, davant dels supòsits de nova incorporació laboral, l'assignació dels codis i de la contrasenya s'efectua a requeriment previ del Departament de Recursos Humans cap l'àrea d'informàtica, que notificarà l'alta corresponent a l'usuari i li facilitarà la contrasenya inicial que hauran de canviar amb posterioritat.

El procediment per a la tramitació de les baixes s'instrumenta seguint els mateixos criteris. En aquest supòsit, el Departament de Sistemes procedeix a cursar la inhabilitació dels codis d'usuari.

D'altra banda, per accedir a les dades de l'aplicació del SOCIAL SIC i de la resta dels programaris es requereix que l'ingrés sigui exercit mitjançant l'autenticació i validació de l'usuari i de la clau de pas.

En qualsevol cas, cal afegir que arrel de la implantació d'aquest circuit, es garanteix que els usuaris només puguin accedir a aquells recursos necessaris per al desenvolupament de les seves tasques.

Àrees de millora

▲	No detectada	

5.12. Identificació i autenticació d'usuaris.

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

Situació actual

Segons el punt 4.4.1 de la Política de Seguretat de la Informació, tot el personal haurà d'accedir als recursos informàtics mitjançant codi d'usuari i contrasenya. Així, la mesura implementada per tal de garantir l'adequada identificació i autenticació dels professionals queda supeditada a l'adjudicació d'un login. D'aquesta manera, cadascun dels treballadors del centre disposa del seu propi nom d'usuari i contrasenya, de forma que l'ingrés al sistema és personalitzat i inequívoc.

Així, la identificació de qualsevol usuari és duu a terme de forma inequívoca i personalitzada, no emprant-se usuaris genèrics o no personalitzats, a excepció dels que es s'enregistren al Reg 09-Llistat d'Usuaris i correus departamentals, on s'identifiquen.

L'Entitat ha optat com a mesura que garanteix la correcta identificació i autenticació dels usuaris l'adjudicació d'un *login* vinculat a un treballador i a una contrasenya inicial que cal ser canviada en el primer accés.

Per a la validació d'un usuari es segueixen, doncs, els següents paràmetres de seguretat:

- Longitud mínima de 8 caràcters.
- Haurà de contenir lletres majúscules, minúscules, números i símbols.
- No podran coincidir amb el codi d'usuari.
- Caducitat corresponent a 6 mesos, no podent-se repetir fins a 14 contrasenyes prèvies.
- Bloqueig per intent d'accés erroni i inactivitat.

D'altra banda, aquestes romanen al sistema emmagatzemades de manera inintel·ligible.

Àrees de millora

▲	No detectada	

5.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

L'apartat 4.4.8 de la Política de Seguretat de la Informació contempla que per a la gestió dels fitxers de nivell alt es guardarà de cada accés la identificació de l'usuari, la data i l'hora, el tipus, la via i el resultat del mateix, així com les dades relatives al fitxer i al registre accedit. Igualment, es determina l'obligació d'emmagatzemar la citada informació durant un termini mínim de dos anys.

A banda, s'atribueix el deure d'efectuar una anàlisi mensual per a detectar possibles problemes de seguretat.

En aquest ordre, l'Entitat ha lliurat un mostreig de l'extracció dels logs extrets durant el mes de febrer i dels informes on es documenten les revisions dels accessos i s'estudia la informació de control i els problemes detectats, acomplint amb això amb els deures que es deriven de l'aplicació de l'article 103.5 del RLOPD.

Àrea de millora

▲	No detectada	

5.14. Còpies de seguretat.

Base legal: Articles 94 i 102 RD 1720/2007

Situació actual

El procediment per a realització de les còpies de seguretat i recuperació de dades apareix definit als punts 4.3.8 i 4.3.9 de la Política de Seguretat de la Informació.

Tot i que cada centre disposa d'un servidor aquests repliquen contínuament el CPD principal que radica al Centre Pilot.

En aquesta línia comentaren que, pel que fa a la còpia local aquesta es realitza de forma diària. A més s'executa una còpia sencera mensual i una setmanal en disc del servidor principal. De les de la resta de centres també es fan còpies setmanals i diàries.

Per altra banda, cada sis mesos es fan proves de restauració de les còpies de seguretat. Així mateix, se'n deixa constància d'aquestes revisions en els informes de verificació semestral del sistema.

Àrees de millora

▲	No detectada	

5.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

En relació als fitxers temporals i considerant que l'Entitat treballa amb un entorn ofimàtic és inherent a l'activitat del centre que es generin aquests tipus de documents. Tanmateix, durant els treballs de camp, l'Entitat informà que, com a regla general, no està permesa la generació d'aquests fitxers i que el personal es troba conscienciat amb aquesta obligació.

Actualment, hi podem trobar determinades referències en tant a aquest tipus d'arxius al punt 4.2.1 de la Política de Seguretat de la Informació i al Manual de Bones Pràctiques.

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 4.2. de la Política de Seguretat de la Informació prediu, pel que fa al transport físic de suports, que a banda d'etiquetar i enregistrar, haurà d'anotar-se qualsevol entrada i sortida de les eines informàtiques en el Reg 03- Entrades i sortides, on s'acompanya el llistat per a la seva anotació, que haurà de dur-se a terme d'acord amb el procediment assenyalat en l'Annex 17.

En relació a l'esmentat, s'observa que el mateix incorpora els paràmetres exigits per l'art. 97 del RLOPD. Addicionalment, a cada centre s'ha establert un responsable que s'encarrega de portar el control emplenant un excel on s'enregistren els moviments corresponents.

En aquest sentit, alguns dels serveis de que disposa l'Entitat; com el de Lleure i Respir, realitzen activitats que requereixen de l'entrada i sortida de suports automatitzats; habitualment, tablets. En aquests casos, tot i que no s'enregistra l'entrada i sortida d'aquests dispositius, des del Departament d'Informàtica sí que es porta un control de la persona encarregada d'exercir la seva custòdia.

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

Les polítiques relatives a la gestió dels suports portàtils apareixen descrites als punts 4.2.4 i 4.2.5 de la Política de Seguretat de la Informació. En aquesta línia, s'informà que els ports USB dels equips es troben habilitats, la política interna de l'Entitat rebutja l'ús de les memòries externes per a l'emmagatzematge de dades.

Paral·lelament, determinats serveis i centres empren càmeres fotogràfiques que són propietat de l' organització per a la captació d'imatges dels usuaris.

Tanmateix, en l'Annex 6-Política d'identificació d'equips es troba definit el procediment per a l'etiquetatge dels equips, havent estat elaborat addicionalment un inventari dels mateixos.

Pel que fa a la destrucció dels suports, en l'Annex 9-Procediment de destrucció i esborrat s'hi estableixen les pautes per a dur a terme l'execució del procés. En aquests termes, en primer lloc es separa el disc dur de la màquina per a ser destruïts físicament amb posterioritat per mitjà d'una radial.

L'Entitat s'ha aprovisionat d'una aplicació d'inventari informàtic anomenada OCS, a parit de la qual s'inventarien de forma automàtica tot els equips. Aquest inventari queda a disposició del responsable d'informàtica.

En relació a la destrucció de la documentació en paper l'Entitat disposa de màquines destructores a cadascun dels centres i a determinats departaments del Centre Pilot, des d'on el personal instrumenta la supressió dels documents quan deixen de ser necessaris per a les seves tasques.

Àrees de millora

▲	No detectada	

5.18. Control d'accés.

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

Situació actual

A la data de realització dels treballs, el CPD roman a la sala dels servidors la qual radica a les instal·lacions del Centre Pilot i es troba dotada d'un sistema de tancament amb clau. A aquesta, només hi té accés el personal del Departament d'Informàtica i, de la mateixa manera es procedeix pel que fa als servidors dels Centres de Teràpia Ocupacional de Badalona o Poblenou.

D'altra banda, es comprovà que les estances i els armaris on s'hi emmagatzema informació sensible, incloent-hi els arxius, disposen de mecanismes de tancament i les claus queden custodiades pel personal amb autorització per a l'accés.

Àrea de Millora

▲	No detectada	

5.19. Registre d'accessos.

Base legal: Article 113 RD 1720/2007.

Situació actual

El punt 4.4.8 de la Política de Seguretat de la Informació preveu la necessitat d'enregistrar els accessos físics a la ubicació on es troben les dades de nivell alt, per part d'aquelles persones no autoritzades. Tal és el cas, dels moviments que es puguin dur a terme en relació a les històries clíniques que romanen en l'arxiu del Centre Pilot.

En aquest sentit, durant els treballs de camp es constatà que tant des d'Admissions; departament al que li ha estat encomanada la tasca d'efectuar el control d'aquests moviments, com també pel que fa al servei de la Residència i Escola, s'està portant un registre dels accessos esdevinguts.

Àrees de millora

▲	No detectada	

5.20. Criteris d'arxiu.

Base legal: Articles 106 RD 1720/2007.

Situació actual

Els criteris d'arxiu garanteixen la correcta conservació de la documentació, la localització i consulta de la informació i possibiliten l'exercici dels drets d'oposició al tractament, accés, rectificació i cancel·lació. En aquest sentit, al punt 4.2.1 de la Política de Seguretat de la Informació es regulen determinats aspectes relatius a la documentació física i, igualment en el Reg 01- Registre de repositoris s'hi preveu una descripció dels suports en format paper, si bé no s'estableixen els criteris d'arxiu emprats. No obstant, durant l'execució dels treballs de camp s'avaluaren aquelles àrees que tracten l'emmagatzematge en paper:

Recursos Humans: Els currículums vitae s'emmagatzemen durant un any al despatx de la responsable de RRHH, endreçats per ordre d'arribada. Pel que fa a l'arxiu laboral actiu, els expedients del personal contractat es troben dins d'un armari tancat amb clau també al despatx de la directora d'àrea, endreçats per ordre alfabètic segons el nom del treballador. El passiu, format per aquells expedients dels treballadors que ja no presten servei a l'Entitat, s'emmagatzema en canvi a una sala a banda, també dotada de mecanisme de tancament amb clau i seguint els mateixos criteris. L'arxiu és custodiat per la responsable de RRHH.

Formació: L'arxiu dels cursos de formació rebuts per part dels treballadors es custodien de forma indefinida al despatx de la responsable de personal, ordenats segons el tipus d'acció formativa.

Facturació i Comptabilitat: Dins el departament d'Administració s'emmagatzema la documentació de l'actiu a un arxiu endreçat per ordre alfabètic del proveïdor i organitzat per anys, fins al 2013. La facturació més antiga, es custodia en el passiu, que s'ubica a una sala independent igualment segons l'ordre alfabètic del proveïdor i l'anualitat. Ambdós són custodiats per part del responsable d'àrea.

Històries clíniques: L'actiu, s'ubica a les instal·lacions de l'Arxiu del Centre Pilot, essent el criteri d'ordenació el del número d'història clínica. La sala roman tancada amb clau i emmagatzema les històries clíniques dels darrers 5 anys, pel que respecta a la vesant assistencial. La custòdia i responsabilitat del mateix recau sobre el Cap d'Admissions.

El passiu, que integra les històries de fa 5 anys en endavant, s'allotja per l'Entitat de gestió MDA en base a uns criteris equivalents als esmentats.

Centres ocupacionals: La documentació que fa referència als usuaris de la resta de delegacions d'Aspace, principalment composta per les anotacions del curs clínic dels pacients, roman als despatxos dels responsables de cada centre, en armaris amb clau i endreçats d'acord amb un criteri alfabètic.

Residencia: Els expedients dels usuaris romanen tancats en un armari amb clau al despatx de la directora, endreçats per nom del pacient. Donada la seva recent creació, encara no s'ha generat arxiu passiu i, per tant, s'hi conserven de forma indefinida.

Escola: Pel que fa als expedients dels usuaris que, addicionalment, esdevenen alumnes de l'escola, els documents de la vessant pedagògica tant de l'arxiu actiu, com del passiu es custodien de

forma indefinida en el despatx de la Direcció del servei endreçats per classe i per l'ordre alfabètic del nom dels usuaris.

Recerca: No existeix pròpiament un arxiu d'investigació clínica com a tal. En aquest sentit, pel que fa a la conservació dels consentiments informats signats pels usuaris i derivats de la realització de possibles estudis d'investigació, aquests s'acoblen de forma conjunta a la història clínica dels pacients. Per aquesta raó, no existeix

Àrees de millora

▲	No detectada	*Tot i que els criteris d'arxiu són correctes, cal que l'Entitat reflecteixi dins dels DDSS corresponents o bé en un protocol annexat a aquest, els criteris emprats o s'hagin de seguir per a l'arxiu de la documentació.*

5.21. Entrades i sortides de documents.

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

Situació actual

L'apartat 4.2.6 de la Política de Seguretat de la Informació regula determinades precaucions a tenir en compte alhora de dur a terme el transport físic de documents.

De la mateixa manera, cal esmentar que gran part d'aquests moviments s'instrumenten des del departament d'Admissions, on disposen d'un registre d'entrada i sortida de la correspondència on hi queda constància del centre, el número, la identificació i el tipus de suport, la data, la forma d'enviament, el contingut, l'emissor i el receptor de l'enviament. Alhora, cadascuna de les delegacions de l'Entitat compta amb el seu propi formulari d'entrades i sortides.

Si més no, tot i que si se'n deixa constància del lliurament dels informes amb els resultats de les proves dels pacients, no s'està duent a terme un control del moviment de les històries clíniques quan aquestes s'extreuen o es retornen a l'Arxiu del Centre Pilot.

Àrees de millora

●	Àrea de millora	Cal que s'enregistrin els moviments de les entrades i sortides de les històries clíniques en suport físic mitjançant un sistema que permeti deixar constància dels paràmetres establerts en l'article 97 del RLOPD: - Tipus de document o suport - Data i hora - Emissor / receptor - Numero de documents o suports - Tipus d'informació que conté - Forma d'enviament / recepció - Persona responsable de recepció / entrega

5.22. Fitxers temporals.

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

Situació actual

Les referències relatives a l'accés, custòdia i destrucció de la documentació en suport paper apareixen contingudes en l'Annex 20-Procediment d'arxius físics de la Política de Seguretat de la Informació.

Tant de la lectura de l'apartat relatiu a la supressió, com arrel de l'execució de les entrevistes i revisions realitzades durant els treballs de camp es pogué constatar que per a la seva eliminació el personal es troba conscienciat en emprar l'ús de les màquines destructores.

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'apartat 5 i l'Annex 14 de la Política de Seguretat de la Informació detallen el procediment per a la notificació, tramitació i resposta davant de les incidències, incorporant en l'Annex 1 els models de llistat on hi queden enregistrades.

Pel que fa a la seva gestió, aquestes són comunicades al Responsable de Seguretat, que mensualment en farà revisions per tal de detectar possibles vulnerabilitats i establir al pla d'acció que resulti adient.

Àrees de millora

	No detectada	

5.24. Difusió de funcions i obligacions.

Base legal: Article 89.2 RD 1720/2007.

Situació actual

Les funcions i obligacions del personal en matèria de protecció de dades venen regulades a la Guia de Bones Pràctiques, que és lliurada al personal d'ASPACE en el moment de la contractació als professionals de nova incorporació. D'aquesta documentació se'n fa signar una còpia, adjuntant-se a l'expedient laboral de cadascun d'ells el rebut com a prova del seu coneixement.

Igualment, al contingut del mateix s'ha definit el règim disciplinari al que estaran subjectes les infraccions, essent aquest el previst pel conveni col·lectiu d'aplicació o el que hi apareix pròpiament regulat a l'Estatut dels Treballadors.

Paral·lelament, s'ha elaborat un Decàleg on es recullen aquells deures bàsics que hauran de ser respectats pels empleats, el qual es troba penjat i a l'abast de tots els departaments i àrees funcionals.

En darrer terme, cal assenyalar que per part del Comitè de Protecció de Dades de l'Entitat s'han dut a terme jornades formatives presencials adreçades a tot el col·lectiu de les que, a més, s'ha portat un registre d'assistències.

Àrees de Millora

▲	No detectada	

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
5.6 Legitimació de dades
III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS
5.21 Entrades i sortides de documents

Barcelona, 27 d'abril de 2017.

Pere Ruiz

- Soci-