ASSOCIACIÓ CENTRE D'HIGIENE MENTAL NOU BARRIS

INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Número de Protocol 10.973

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 mig 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 Centre d'Higiene Mental Nou Barris
NIF	G08725665
Domicili	Passeig Valldaura, 214, baixos 08042 Barcelona

3.1.2. Descripció de l'activitat

L' ASSOCIACIÓ CENTRE D'HIGIENE MENTAL NOU BARRIS és una entitat sense ànim de lucre, creada l'any 1995.

L'objectiu de la seva creació és desenvolupar i promoure activitats dins de l'àmbit de la salut mental.

L' Entitat per tal d'assolir l'objectiu realitza les següents activitats, entre d'altres:

a) L' Associació i els equips que gestiona es coordinen amb entitats ja siguin culturals, familiars, etc. i professionals relacions amb el fi de l' Associació.
b) L' associació realitza formació de salut mental comunitària a metges de família, MIR Psiquiatria, PIR, psicòlegs en formació, escoles de Treball Social , etc.
c) L' associació te línies obertes d'investigació.
d) L'associació col·labora amb organismes públics relacions en l'àmbit d'actuació de l' Entitat.

3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els diversos serveis i àrees de l' Associació Centre d' Higiene Mental Nou Barris:

En el CSM Nou Barris Sud, els treballs de camp s'han realitzat en les següents àrees:

- Àrea de Sistemes d' Informació.
- Àrea d' Arxiu de Documentació Clínica.
- Àrea d'Admissions.
- Àrea de Recursos Humans i Salut Laboral.
- Àrea d'Administració.
- Àrea de Comunicació.
- Àrea Assistencial.

En el CSM Nou Barris Nord, s'han visitat les següents àrees:

- Àrea Assistencial.
- Àrea d'Admissions.
- Àrea d' Arxiu de Documentació Clínica.

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

3.2.1. Data de realització de l'auditoria

Dia	23 i 24 d'abril

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

Persones entrevistades per ordre d'intervenció:

NÚMERO	PERSONA ENTREVISTADA	ÀREA DE TREBALL
1	Sr. Ferran González	Cap d'Administració i Gestió dels CSM Nou Barris Nord i Sud
2	Sra. Meritxell Hernández	Administració CSM Sud
3	Dr. Francisco Porras	Cap clínic CSM Sud
4	Sra. Miquel Moya	Responsable d'Informàtica
5	Sra. Ana María Fernández	Administració CSM Nord

Relació de la documentació lliurada a l'auditor:

Organigrama
Estatuts
Cartes de l'Agència Espanyola de Protecció de Dades amb els codis d'inscripció dels fitxers
Documents de seguretat
Esquema xarxa informàtica
Document d'usuaris, permisos i inventari
Altes i baixes d'usuaris
Relació d'usuaris autoritzats d'accés a les dades
Registre contractes

Protocol xifrat arxius
Annexes documentació informació (pacients, treballadors, etc...)
Protocol exercici drets ARCO
Contractes
Model de clàusula sobre la prestació de serveis sense accés a dades
Procediment de gestió i registre d'incidències
Taula d'incidències informàtiques
Sol·licitud i recollida d'HC per persona diferent a l'interessat
Acta Comitè de Direcció i Ordre del dia
Certificat de document entregat
Sol·licitud primera visita de persona diferent a l'interessat
Acta de tancament d'auditoria

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

L'Associació Centre d'Higiene Mental Nou Barris, en endavant l'Entitat, realitzà l'anterior auditoria en matèria de protecció de dades el setembre de 2016, conforme a les previsions que estableix la legislació en protecció de dades. Amb la present auditoria es dóna compliment al requeriment de la biennalitat en la realització de les auditories.

Entre la documentació aportada per l'Entitat, consta que les conclusions de la darrera auditoria van ser elevades a la Direcció de l'Entitat per tal d'adoptar les mesures correctores adequades.

Àrees de millora

▲	No detectada	

5.2. Aspectes generals.

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

Situació actual

De la consulta al Registre de l'Agència Espanyola de Protecció de Dades, consta que a data de la present Auditoria, l'entitat té registrats els següents fitxers:

FITXER	CODI	FINALITAT	NIVELL	TRACTAMENT
Pacients	2031880119	Prestació de prevenció i d'assistència sanitària, facturació dels serveis prestats, així com també finalitats de docència i investigació epidemiològica i activitats anàlogues	Alt	Mixt
Personal	2031890468	Gestió de recursos humans, formació, prevenció de riscos laboral i control presencial dels treballadors.	Alt	Mixt
Administració	2031890467	Realitzar els processos habituals d'administració i comptabilitat.	Bàsic	Mixt

Àrees de millora

▲	No detectada	**Observació d'acord al nou RGPD:** D'acord a la nova legislació, la declaració dels fitxers no serà necessària però, no obstant això, aquests es converteixen en Activitats de Tractament les quals s'han de transcriure en un registre d'acord l'article 30 del RGPD. Es considera necessari tenir correctament regulats els fitxers per l'efectiu trasllat com a activitats de tractament.

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 disposa d'un Document de Seguretat per cadascun dels fitxers inscrits: Pacients, Personal i Administració, tot i que aquests no es troben degudament aprovats pel Responsable dels Fitxers. • L' última versió de tots els DDSS és del 18 d'agost de 2017, sent la v.4 pel DS de Pacients, la v.2 pel DS d'Administració i la v.3 pel DS de Personal.
B. Àmbit d'aplicació del document amb especificació detallada dels recursos protegits: o Inventari de suports. o Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten.
Comentaris: • L'Entitat disposa d'un inventari de suports com annex dels DDSS • En el punt 2 de tots els DDSS es descriu l'estructura dels fitxers, exposant-se la descripció dels sistemes d'informació que els tracten.

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: • En els DDSS s'estableixen mesures de seguretat que, com a mínim, donen compliment a la normativa en matèria de protecció de dades d'acord amb el nivell de seguretat establert. Malgrat tot, no s'ha detectat la necessitat de fer constar mesures de seguretat alternatives, doncs és possible implementar aquelles previstes per la normativa.
D. Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit en el Reglament.
Comentaris: • L'Entitat disposa de protocols i procediments com són el procediment d'altes i baixes d'usuari, gestió i registre d'incidències, encriptació de documents, protocol per a l'exercici de drets ARCO, etc.
E. Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers.
Comentari: • Els DDSS de Pacients i Personal incorporen el Manual de Bones Pràctiques de l'Entitat, on s'inclouen les funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal, així com les sancions en cas d'incompliment.
F. Procediment de notificació, gestió i resposta davant les incidències.
Comentari:

- L'Entitat estableix un procediment de notificació, gestió i resposta davant les incidències en el punt 5.8.3 del DS de Pacients, en el punt 5.6.2 del DS de Personal i en el punt 5.4.1 del DS d'Administració.
- Així mateix, es disposa d'un document com annex als DDSS on es detalla amb més profunditat el procediment de notificació i gestió del registre d'incidències.

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

Comentari:

- Es troba regulat en el punt "Procediment, periodicitat i custòdia per a la realització de còpies de seguretat" del DS de Personal i Administració. Manca regular-ho en el DS de Pacients.
- En cap dels DDSS es fa menció a les proves de recuperació de dades.

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:

- Cal incorporar les mesures necessàries per al transport de suports i documents. S'hi fa una petita menció en el Manual de Bones Pràctiques.
- Es preveu la destrucció de documents a través de la màquina trituradora dins de les mesures respecte a les dades en suport físic en Manual de Bones Pràctiques incorporat en els DDSS de Pacients i Personal.

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

Comentaris:

- En el DS d'Administració trobem el llistat incomplet en el punt *Descripció de les obligacions dels usuaris i tercers amb accés a les dades*. Tot i així, s'hauria de completar i incloure'l a la resta de DDSS, o bé, com annex a tots als DDSS.

J. Quan l'entitat actuï com a encarregat de tractament en els seus propis locals, aliens als del responsable del fitxer, ha de preveure en els documents de seguretat oportuns la identificació del fitxer o tractament i el seu responsable i les mesures de seguretat a implementar en relació amb el tractament.
Comentari: • No queda constància que actuï com a encarregat de tractament de terceres entitats.
Autoritzacions
K. Autorització per a l'emmagatzematge de dades de caràcter personal en dispositius portàtils (usuaris/ perfils d'usuaris i període de validesa). Tractament de dades de caràcter personal en dispositius portàtils que no permetin el xifratge.
Comentari: • En el Manual de Bones Pràctiques es regula l'ús dels dispositius d'USB. Durant els treballs de camp es comentà que els ports es tan habilitats i que no estava prohibit el seu ús. Cal adaptar el Manual de Bones Pràctiques a la realitat de l' Entitat i, si cal, autoritzar al personal corresponent per la utilització d'aquests dispositius.
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: • No consta cap referència respecte al tractament de dades de caràcter personal fora dels locals del responsable en caps dels DDSS de l'Entitat.
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:

• No es preveu el personal autoritzat per concedir, alterar o anul·lar l'accés sobre els recursos. Es recomana incloure-ho en un protocol.
N. Personal autoritzat a accedir als llocs on estiguin instal·lats els equips físics que donin suport als sistemes d'informació. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.
Comentari: • Aquests consten en el punts 5.5 *Control i Limitació d'accés físic*, del DS del fitxer de pacients i personal.
O. Personal autoritzat a accedir als suports i documents que contenen dades de caràcter personal. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.
Comentari: • En el punt 5.2.1 del DS d' Administració i el 5.3.1 de Pacients i Personal es preveu un llistat de persones autoritzades a l'accés a dades. Així mateix, es disposa d'un document de *Relació dels usuaris autoritzats d'accés a les dades,* identificant el tipus d'accés al qual està autoritzat.
P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.
Comentaris: • No es preveuen en cap punt les autoritzacions per a les sortides de suports i documents, així com els annexos a un correu electrònic. Cal detallar-ho per exemple en forma de protocol.
Q. Personal autoritzat per a la recepció/ enviament de dades de caràcter personal *(nivell mitjà i/ o alt)*.
Comentari: • No es preveu en cap punt el personal autoritzat per a la recepció/enviament de dades de caràcter personal (nivell mitjà/alt).
R. Personal autoritzat per a la realització del procediment de recuperació de dades.

Comentari: • En cap dels DS s'especifica ni el procediment de recuperació de dades ni la persona responsable de dur-la a terme.
S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.
Comentaris: • Veure punt 5.4 del present informe.
Altres mesures
T. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat.
Comentari: • No es preveu en cap dels DDSS un procediment d'assignació, distribució i emmagatzematge de contrasenyes que garanteixi la confidencialitat i la integritat.
U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.
Comentari: • En els punts 5.3.2 dels DDSS de Pacients i de Personal i en el punt 5.2.2 del DS d'Administració relatiu a la *Descripció de les obligacions dels usuaris i tercers amb accés a les dades* es determina la caducitat de les contrasenyes per un període de 90 dies.
V. Pel cas que es realitzin proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal amb dades reals s'ha d'anotar la seva realització al document de seguretat.

Comentari: • No consta que es realitzin proves amb dades reals.
W. Identificació del responsable de seguretat *(nivell mitjà i/ o alt)*.
Comentari: • Aquest consta en el punt *El Responsable de Seguretat*, en el punt 5.2 del DS de Pacients i de Personal. Manca fer-ho constar en el DS d'Administració.
X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt)*.
Comentari: • Els DDSS de Pacients i de Personal estableixen que una de les funcions del responsable de seguretat és coordinar i controlar el compliment de les mesures de seguretat. Així mateix, s'indica que haurà de revisar cada mes la informació de control registrada i el funcionament del sistema amb el que elaborarà un informe de les revisions realitzades i els problemes detectats.

Àrees de millora

●	Àrea de millora	Cal que l'Entitat corregeixi els punts comentats en el quadre anterior i que adapti els diferents DDSS de Pacients, Personal i Administració a la seva realitat.

5.4. Delegació d'autoritzacions.

Base legal: Article 84 RD 1720/2007.

Situació actual

Entre la documentació aportada per l'Entitat trobem el document *Responsables Protecció de dades* on s'indiquen les delegacions que el responsable del fitxer realitza sobre persones a qui s'assignen funcions i tasques específiques.

En aquest document s'indica que el Responsable dels Fitxers és la Directora dels Centres de Salut Mental dels Centres Nou Barris Nord i Sud. Pel que fa al Responsable de Seguretat d'ambdós centres és el Cap d'Administració i Gestió dels Centres de Salut Mental Nou Barris Nord i Sud.

Les funcions que es deleguen al Responsable de Seguretat es troben establertes en el DS en el seu punt 5.2 on s'indica que és l'encarregat de coordinar i gestionar les mesures de seguretat definides pel responsable del fitxer. Així doncs, les seves funcions són:

- Coordinar i controlar el compliment de les mesures de seguretat.
- Supervisió del registre d'incidències.
- Revisió mensual dels registres.
- Elaboració d'informes d'incidències, els quals seran analitzats a la Junta de l'Associació.
- Anàlisi dels informes d'auditoria.

Per altra banda, en el punt 5.3.2 del DS es preveuen les obligacions dels usuaris i tercers amb accés a les dades establint la confidencialitat de les dades i les mesures de prevenció per garantir aquesta confidencialitat.

Àrees de millora

▲	No detectada	**Observació d'acord al nou RGPD:** L'entrada en vigor de la reglamentació europea obliga a l'Entitat a la designació d'un Delegat de Protecció de Dades d'acord als articles 37 i següents. D'acord als criteris de les Agències aquesta figura haurà d'estar ja designada a data 25 de maig del 2018.

5.5. Tercers.

ENCARREGATS DE TRACTAMENT

Base legal: Article 82 RD 1720/2007.

Situació actual

Un cop realitzat el mostreig dels contractes facilitats per l'Entitat, es passen a analitzar els següents:

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
ASTIM INFORMÀTICA, SR.L.L.	Manteniment de sistemes d'informació	☑	L'Entitat disposa d'un contracte d'encarregat de tractament conforme a l'article 28 del RGPD.
BLÀZQUEZ PLANAS I ASSOCIATS, S.L.	Assessoria laboral, gestió de nòmines, tramitació d'assegurances socials i assessoria fiscal i comptable	☑	L'Entitat disposa d'un contracte d'encarregat de tractament conforme a l'article 28 del RGPD.
29 ECOLÒGICA, S.L.U.	Recollida i destrucció de contenidors de documentació confidencial, paper i cartró	☑	L'Entitat disposa d'un contracte d'encarregat de tractament conforme a l'article 28 del RGPD.
Fundació Hospital de Dia Nou Barris i Fundació Nou Barris per a la Salut Mental	Col·laboració entre les tres entitats	☑	Es disposa del contracte d'encarregat de tractament d'acord amb les previsions de l'article 12 de la LOPD, si bé cal detallar les mesures de seguretat aplicables en cada cas.
SEPRA	Prevenció de Riscos Laborals i Vigilància de la Salut	☑	L'Entitat disposa d'un contracte d'encarregat de tractament conforme a l'article 28 del RGPD.

Àrees de millora

▲	No detectada	**Observació d'acord al nou RGPD:** A partir del 25 de maig de 2018 els contractes ja signats, i els darrers, amb els Encarregats dels Tractaments hauran de respectar el contingut que preveu l'article 28 del RGPD.

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

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

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS	COMENTARIS
CLECE, S.A	Neteja del CSM Nord	☑	El contracte de prestació de serveis facilitat incorpora en la seva clàusula 14ª el compromís de confidencialitat d'acord amb l'article 83 del RDLOPD.
ISS FACILITY SERVICES, S.A	Neteja del CSM Sud	☒	L'Entitat ha aportat un contracte d'encarregat de tractament. Atès que aquest tercer no té o no ha de tenir accés a dades per la prestació del servei, és necessari que es signi un compromís de confidencialitat.

Àrees de millora

●	Àrea de millora	És necessari que l'Entitat signi un compromís de confidencialitat amb tots aquells tercers que, si bé per a la prestació del servei no han d'accedir a les dades que s'inclouen en els fitxers de l'Entitat, sí que accedeixen a les instal·lacions de l'Entitat podent tenir accés en casos fortuïts. És important que el model de compromís de confidencialitat que s'utilitzi des de l'Entitat compleixi amb els requisits de l'article 83 del RD 1720/2007. Així doncs, aquest hauria d'incloure els dos aspectes que preveu l'article: per una banda, la prohibició d'accés a les dades per a la prestació del servei objecte del contracte i, per una altra, el deure de secret en cas d'accés fortuït a dades gestionades per part de l'Entitat.

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
Administració	Les dades tractades en el marc de l'activitat d'administració de l'Entitat no tenen caràcter personal, o bé, procedeixen d'altres fitxers.	La facturació a proveïdors emesa per part del departament d'Administració no suposa la recollida de dades de caràcter personal.
Pacients	L'Entitat disposa d'un document d'informació i consentiment per a l'enviament de SMS de recordatoris de visites.	El document facilitat es troba adaptat al RGPD. Tot i així, cal fer unes matisacions com són que el Responsable de Tractament és la pròpia Entitat i; pel que fa a la cessió de dades al HC3 no és necessari demanar el consentiment als pacients atès que aquesta cessió està habilitada per llei.
	Els pacients que volen demanar un informe assistencial han d'omplir un el document "*Petició d'informe assistencial" per* l'interessat un cop desitja fer la petició i també per a la recollida fent constar que s'ha entregat a l'interessat.	La clàusula que incorpora el present document és conforme a l'article 13 RGPD.
Personal	Quan entra un nou treballador se li entrega el document per signar *"Full d'informació i confidencialitat*	Aquest document és correcte d'acord amb l'article 5 de la LOPD.

	de l'empleat". Igualment se li entrega el Manual de Bones Pràctiques.	
	Els estudiants en pràctiques i voluntaris també signen un document de confidencialitat en el tractament de dades de caràcter personal.	Aquest document, a banda de preveure el deure de secret de l'article 10 LOPD, és correcte d'acord amb l'article 5 relatiu al dret d'informació en la recollida de dades.
	Els treballadors han de donar el seu consentiment pel reconeixement mèdic en el *"Document d'informació i consentiment a l'examen de salut dels treballadors".*	Aquest document és correcte d'acord amb l'article 5 de la LOPD.
	L'Entitat disposa d'un model de resposta per a la recepció de CV per tal de legitimar les dades de caràcter personal dels candidats.	El document és correcte per tal de legitimar les dades dels candidats.

Àrees de millora

●	Àrea de millora	L'Entitat no ha de demanar el consentiment pel que fa a la cessió de dades de pacients en el sistema d'Història Clínica Compartida de Catalunya (HC3), pel fet de que existeix una habilitació legal per aquesta cessió. Tanmateix, sí és necessari el consentiment per l'enviament de SMS a pacients, atès que aquesta activitat no pertany a l'activitat assistencial. Cal dir també que la Paloma Lago no és la Responsable del Tractament, sinó que ho és la pròpia Entitat. **Observació d'acord al nou RGPD:** Segons els criteris manifestos per les diferents Agències, les institucions que encara que hagin legitimat correctament les dades a partir de l'article 5 de la LOPD requeriran que amb l'entrada en vigor de la normativa europea legitimin totes les dades que tracten a partir dels articles 13 i 14 del RGPD. S'aconsella a l'Entitat la revisió de les clàusules d'acord la normativa europea.

5.7. Drets ARCO.

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

Situació actual

L'exercici de drets ARCO està previst en el punt 6.1 dels DDSS. Així mateix, s'annexa un *Protocol Drets ARCO* per tal de definir el procediment a seguir en quant al compliment dels articles 13 i següents de la LOPD relatius a l'exercici de drets.

Durant l'entrevista amb la responsable del departament d'Administració i Admissions del CSM Nord, es constatà que hi havien hagut dues peticions d'exercici del dret d'accés en l'últim any, havent-se donat resposta el dia següent a la sol·licitud en ambdós casos.

Es constatà que l'Entitat no considera un dret d'accés la petició d'informe, havent-se d'omplir el formulari específic de petició d'informes. En el cas que la petició la faci un tercer, se li demana la documentació pertinent per tal d'acreditar la seva vinculació amb l'interessat.

Durant l'entrevista amb la Cap d'Administració del CSM Nord, es constatà que es dona resposta dins del termini legalment establerts. Així doncs, es va constatar que una sol·licitud s'havia realitzat el 14 de març i es va donar resposta el dia 22 del mateix mes. D'aquesta manera, es constatà que es compleixen els terminis de resposta tant en el CSM Nord com en el CSM Sud.

Pel que fa al dret de rectificació, ens comentaren que la gestió es realitza sense demanar a l'interessat que ompli el corresponent formulari, modificant les seves dades directament des del sistema d'informació de manera immediata.

També es constatà que l'Entitat (tant en el CSM Nord com en el CSM Sud) no porta a terme un registre de les peticions d'exercici d'aquests drets, tot i que comentaren que es podria extreure indirectament pel fet de que es guarden de manera digitalitzada.

Àrees de millora

▲	No detectada	Recordar que pel què fa a l'exercici dels drets ARCO a la història clínica compartida de Catalunya (HC3), l'Entitat ha de subjectar-se al que es disposa en el protocol específic: http://aquas.gencat.cat/ca/detall/article/protocol_drets_acces_hc3 **Observació d'acord al nou RGPD:** A més de considerar la modificació de les clàusules de legitimació de dades d'acord l'article 13 del RGPD, l'Entitat ha de tenir en compte les modificacions entorn dels terminis de resposta (art. 12.3 RGPD) i la regulació dels nous drets (art. 15 al 22 del RGPD)

II - BLOC DE MESURES INFORMÀTIQUES

5.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'Entitat disposa de dos servidors, dels quals un és de domini l'altre allotja el correu electrònic. La connexió entre els dos CSM es realitza per VPN amb ADSL de 6mb, tot i que ens comentaren que està previst que arribi per fibra òptica.

El responsable d'Informàtica de l'Entitat comentà que tots els ordinadors disposen de l'antivirus NOD32 i d'un Firewall que és gestionat per Astim Informàtica, el seu proveïdor informàtic. També es constatà que l'Entitat disposa d'un SAI que es troba a la sala del servidor.

Durant els treballs de camp, es constatà que l'Entitat disposa d'un sistema de carpetes, en el qual hi ha una unitat central on té accés tot el personal amb usuari i contrasenya al sistema informàtic, una unitat comuna per cada un dels CSM Nord i Sud i, a més carpetes departamentals on tenen accés els usuaris de cada departament i carpetes personals.

L'Entitat utilitza Microsoft Exchange pel correu electrònic dels treballadors, els quals disposen d'un compte de correu electrònic amb usuari i contrasenya.

Les aplicacions detectades durant el treball de camp utilitzades per l'entitat i en les quals es tracten dades de caràcter personal es detallen a continuació:

APLICACIÓ	UTILITAT
EKON	Gestor assistencial
Control de derivacions i ingressos	Gestor de derivacions d'usuaris
Microsoft Exchange Server	Gestor de correu electrònic
Microsoft Office	Programes ofimàtics

Àrees de millora

▲	No detectada	

5.9. Connexions remotes.

Base legal: Article 86 RD 1720/2007.

Situació actual

Les connexions remotes estan previstes en cap dels DDSS d'Administració, de Personal i de Pacients, els quals estableixen que els proveïdors informàtics, Isalus i Astim Informàtica seran els únics agents externs que podran accedir remotament a les dades a través de l'*Any Desk* amb una IP facilitada pel departament d'Informàtica.

També es preveu que l'accés sigui d'un sol ús i prèviament es demanarà permís al departament d'Informàtica per poder iniciar la connexió remota. Tanmateix, l'Entitat no disposa d'un protocol que estableixi el procediment que es segueix per autoritzar aquests accessos.

Durant els treballs de camp, ens comentaren que està previst la implementació de connexions remotes pels treballadors d'atenció domiciliària de l'Entitat.

Àrees de millora

●	Àrea de millora	Cal que l'Entitat estableixi en un protocol quin és el procediment intern que es segueix per tal d'autoritzar aquests accessos remots.

5.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

L'Entitat disposa del document *"Procediment d'encriptació de documents"* com a protocol per a encriptar documents mitjançant l'eina ofimàtica Open Office. El responsable informàtic de l'Entitat comentà que l'encriptació amb contrasenya també es pot realitzar directament a través del programa de gestor assistencial *EKON*.

El punt 5.7 del DS de Pacients preveu l'ús de l'eina Open Office 4.1.2 per l'encriptació dels documents amb dades personals i de salut en la transmissió d'informació que contingui dades de caràcter personal per correu electrònic. De la mateixa manera, el Manual de Bones Pràctiques preveu l'encriptació d'aquests documents quan s'enviïn per correu electrònic.

Durant les diferents entrevistes mantingudes amb el personal de l'Entitat, es constatà que tots els treballadors amb accés a dades de caràcter personal utilitzen aquesta eina degudament per a l'enviament de dades per correu electrònic.

Es constatà que en tots aquests, la contrasenya es facilita en correu electrònic a banda.

Pel que fa a l'ús del fax, durant les entrevistes amb les responsables d'Administració d'ambdós CSM es constatà que alguna vegada s'utilitza per a l'enviament d'informació que requereixen els Jutjats, tot i que es fa de manera dissociada, sense fer constar el nom del pacient. Tot i això, en aquests casos que es realitzen enviaments per requeriment de Jutjats es fa constar en el registre d'incidències que disposa l'Entitat.

Àrees de millora

▲	No detectada	

5.11. Control d'accés.

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

Situació actual

En el DS de Pacients s'estableix un llistat dels treballadors amb accés a les dades de l'*EKON*, on s'identifica l'usuari, el càrrec que ostenta, el centre al qual pertany i el tipus d'accés.

El responsable informàtic comentà que l'accés a les dades del programa *EKON* es troba limitat segons el seu càrrec (administratius, psiquiatres, tècnics, etc.).

Pel que fa a les altes i baixes d'usuaris, l'Entitat disposa d'un protocol on es detallen els passos a seguir per a cadascun dels procediments.

Així doncs, pel que fa al procediment d'alta de nous usuaris, s'envien les dades del nou usuari al responsable de la gestió d'usuaris del sistema informàtic (Astim Informàtica), el qual donarà d'alta amb un nou compte i una contrasenya diferent, assignant els permisos corresponents per poder accedir a les carpetes de documents que ha d'utilitzar per a les seves funcions.

En quant al procediment de baixa d'usuaris, s'envien les dades de l'usuari que s'ha de donar de baixa al responsable de la gestió d'usuaris del sistema informàtic (Astim Infosmàtica). Es procedeix a eliminar el compte d'usuari en el sistema, desactivant-ne la bústia de correu i mantenint l'usuari inactiu durant 30 dies, transcorreguts els quals s'esborra definitivament.

Durant l'entrevista amb el responsable informàtic, es constatà que la baixa d'usuaris de l'*EKON* és immediata.

Àrees de millora

▲	No detectada	

5.12. Identificació i autenticació d'usuaris.

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

Situació actual

Per tal de garantir la correcta identificació autenticació dels usuaris, tot el personal amb accés al sistema i als programes disposa d'usuari i contrasenya.

Pel que fa a l'accés al Windows, cada treballador disposa d'un usuari i contrasenya, la qual li permet accedir al programa propi de Control de derivacions i ingressos. La contrasenya ha de contenir 8 dígits, ha de ser alfanumèrica amb un símbol i caduca cada dos mesos.

Pel que fa al programa de gestió assistencial *EKON*, es constatà que la contrasenya ha de ser també de 8 caràcters alfanumèrics, caduca cada dos mesos i es bloqueja als cinc intents erronis, no podent utilitzar les últimes 25 contrasenyes per modificar la contrasenya.

Àrees de millora

▲	No detectada	

5.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

Tant el DS de Pacients com el de Personal preveuen l'existència d'un Registre d'accessos, per tal de controlar l'ús i la confidencialitat de les dades. S'indica que de cada accés es guardaran com a mínim la identificació de l'usuari, la data i hora en què es va realitzar, el fitxer accedit, el tipus d'accés (consulta o modificació) i si l'accés es va autoritzar o denegar.

Durant l'entrevista amb el responsable informàtic de l'Entitat, es constatà que no es porten a terme revisions mensuals dels accessos registrats en els diferents programes que utilitza el personal de l'Entitat.

L'Entitat ha aportat un informe de les revisions realitzades pel que fa als accessos a les històries clíniques durant el mes de juny. Tot i així, no es pot constatar que les revisions dels accessos realitzats es portin a terme de manera mensual.

Àrees de millora

●	Àrea de millora	Cal que l'Entitat porti a terme revisions dels accessos produïts en els diferents sistemes d'informació dels que disposa i elaborar un informe de les revisions realitzades, almenys una vegada al mes, tal i com estableix l'article 103 RLOPD.

5.14. Còpies de seguretat.

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

Situació actual

El punt 5.3.3 del DS d'Administració i el punt 5.2.3 del DS de Personal descriuen el procediment, la periodicitat i la custòdia per a la realització de còpies de seguretat. Així doncs, es preveu la còpia total cada dia 1 de cada mes i dues còpies incrementals diàries (al migdia i a la nit).

Durant els treballs de camp, es constatà que les còpies de seguretat són gestionades pel proveïdor informàtic de l'Entitat, Astim Informàtica. Ens comentaren que les còpies es realitzaven al servidor intern de l'Entitat i d'allà s'enviaven a un servidor extern gestionat pel proveïdor informàtic, complint així amb l'obligació legal d'externalització de les còpies de seguretat pels fitxers que contenen dades de caràcter personal de nivell mig/alt.

També ens comentaren que pel que fa a les dades contingudes en el programa de gestió assistencial (EKON), la còpia es realitza directament al TecnoCampus de Mataró i es fa arribar una còpia al servidor intern de l'Entitat via FTP.

Totes les còpies de seguretat, tant les que es realitzen en el servidor intern de l'Entitat com les que es realitzen al TecnoCampus de Mataró es graven amb disc dur.

Pel que fa a les proves de recuperacions de dades, l'Entitat ha aportat un mostreig dels informes de les últimes proves de recuperació de dades que s'han realitzat per part del proveïdor informàtic, complint així amb el que preveu la normativa vigent en matèria de protecció de dades.

Àrees de millora

▲	No detectada	

5.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

El Manual de Bones Pràctiques fa menció a la creació de fitxers temporals en suports automatitzats per la realització de treballs temporals, els quals hauran de complir un nivell de seguretat. Així doncs, s'indica que aquests s'hauran d'esborrar o eliminar una vegada deixin de ser necessaris.

Respecte l'ús de l'USB, també es fa menció en el Manual de Bones Pràctiques indicant que els ports per aquests dispositius es troben inhabilitats i seran utilitzats única i exclusivament amb la finalitat de la prestació dels serveis i tasques de l'Entitat, garantint el compromís de confidencialitat i l'ètica professional.

Durant els treballs de camp, es constatà que tots els ports USB es trobaven habilitats i no està prohibit l'ús de l'USB pel personal de l'Entitat. Tot i això, no es detectà que el personal de l'Entitat treballés amb documents dels que no es fes còpia d'aquests a les carpetes en xarxa del servidor ni tampoc que arxius temporals quedessin guardats fora dels llocs que ofereixen seguretat.

Àrees de millora

▲	No detectada	

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

Base legal: Article 97 RD 1720/ 2007.

Situació actual

El DS de Pacients en el seu punt 5.8.1 determina l'existència d'un Registre d'entrades i sortides de suports en format físic, tot i que el model de registre que s'annexa fa referència a les entrades i sortides de suports tant físics com automatitzats.

L'Entitat ha aportat el registre d'entrades i sortides de suports que disposa, en el qual consta un sol enviament. L'Entitat indicà que aquest procediment es troba en actiu des de fa poc.

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

L'Entitat disposa del corresponent inventari de suports en un document Excel en qual es detallen tots els equips informàtics dels que disposa l'Associació Centre d'Higiene Mental Nou Barris. En aquest llistat els equips estan ordenats per un número on es fa referència de la ubicació, la descripció, la marca, el model, el tipus de CPU, la capacitat RAM i HD, i el sistema operatiu.

D'aquest llistat es desprèn que l'Entitat disposa actualment d'aproximadament 50 suports, entre ells els servidors, els ordinadors portàtils i els ordinadors de sobretaula. Durant els treballs de camp, ens comentaren que aquests dispositius no es trobaven assignats a uns professionals concrets, sinó que són compartits pels diferents professionals de l'Entitat. El responsable del departament d'Informàtica comentà que aquest llistat és elaborat per Astim Informàtica.

Es comentà que no es té constància de la utilització de dispositius USB encara que els ports es trobin habilitats.

Durant els treballs de camp es constatà que per a la destrucció de suports, el proveïdor Astim Informàtica els recull i els destrueix a les seves instal·lacions. L'Entitat ha aportat un certificat conforme aquest proveïdor ha destruït correctament el suport.

Pel que fa la destrucció de documentació, és l'empresa externa 29 Ecològica, S.L.U. l'encarregada de recollir i destruir la documentació física.

Àrees de millora

▲	No detectada	

5.18. Control d'accés.

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

Situació actual

El servidor de l'Entitat es troba en una sala darrere del taulell d'Admissions del CSM Nou Barris Sud on es troba també l'arxiu d'històries clíniques i també s'utilitza com a magatzem per desar material d'oficina.

L'accés a aquesta sala es realitza mitjançant contrasenya i ens comentaren que només hi tenia accés el personal d'Administració, el personal assistencial i Informàtica per accedir al servidor. Així mateix, ho determina el DS de Personal en el seu punt 5.5.

Els fulls de queixes i reclamacions es guarden en una prestatgeria fora d'aquesta sala i no es troba tancada amb clau ja que està en el mateix taulell d'Admissions. Ens comentaren que estava així de manera provisional ja que s'estaven realitzant obres en el taulell durant els dies en què es varen realitzar els treballs de camp.

En el CSM Nou Barris, les històries clíniques es troben en una sala que s'accedeix amb codi i ens comentaren que només té accés el personal d'Administració i el personal assistencial.

Tota la documentació referent al departament de Recursos Humans es troba en un armari tancat amb clau dins del despatx d'Administració, tenint accés només el Cap d'Administració de l'Entitat. Pel que fa a la documentació relativa a la contractació i facturació de l'Entitat es troba es troba també al despatx d'Administració en un altre armari que queda tancat amb clau, tenint accés el Cap d'Administració i la Directora de l'Entitat.

Àrees de millora

▲	No detectada	

5.19. Registre d'accessos.

Base legal: Article 113 RD 1720/2007.

Situació actual

El Manual de Bones Pràctiques tan sols fa referència al registre d'accessos a les històries clíniques informatitzades, però res s'esmenta sobre els accessos a les històries clíniques i a la documentació amb dades personals en format paper. De la mateixa manera ho estableix el DS de Pacients en el seu punt 5.8.2.

Durant els treballs de camp es constatà que tant el CSM Nou Barris Nord com el CSM Nou Barris Sud no disposen de mecanismes que permetin identificar els accessos realitzats com són els diferents arxius dels quals disposa l'Entitat.

Tot i així, l'Entitat preveu en el Document de Seguretat l'ús de codi per part del personal per tal d'accedir a la sala on s'ubiquen les històries clíniques.

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'accés, rectificació, cancel·lació i oposició al tractament:

Arxiu d'Històries Clíniques: l'Entitat divideix l'arxiu d'històries clíniques entre els dos centres, el CSM Nou Barris Nord i Sud. En el cas del CSM Nou Barris Sud es troba ubicat en una sala just darrere del taulell d'Admissions tant per l'arxiu actiu com per l'arxiu passiu i s'ordenen per any de creació i número d'història clínica. En el CSM Nou Barris Nord es segueix el mateix criteri d'ordenació i es troba en una sala ubicada al despatx d'Administració.

Arxiu de Queixes i Reclamacions: les queixes i reclamacions es guarden en el CSM Nou Barris Nord i s'ubiquen en una prestatgeria al taulell d'Admissions i s'ordenen per la data de recepció.

Arxiu de Facturació i Contractació: pel que fa als contractes de prestació de serveis amb els diferents proveïdors de l'Entitat es guarden en un armari dins del despatx del Cap d'Administració i s'ordenen pel tipus de servei prestat. Pel que fa als contractes relatius a LOPD també es guarden a banda.

En quant a les factures del departament de Facturació es guarden en el despatx del Cap d'Administració dins d'un armari i s'ordenen per mesos des del 2010. La resta que són més antigues es guarden fora de l'armari ordenades amb arxivadors per anys.

Arxiu de Recursos Humans: es troba en el mateix despatx del Cap d'Administració dins d'un armari i es divideixen pel personal que es troba en actiu a l'Entitat i el personal que ja no hi treballa. El criteri d'ordenació és segon l'antiguitat dels treballadors.

Pel que fa als currículums es guarden en el mateix armari dividits per perfils de professionals. També hi trobem una carpeta amb currículums de candidats preseleccionats.

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 programa propi de *Control de derivacions i ingressos* on es registren totes les derivacions i els ingressos que s'envien i es reben a l'Entitat. En aquest programa queda registrat el pacient que es tracta, l'adreça del centre a on es deriva i el tipus de diagnòstic que té el pacient. També queda registrat l'usuari que dona d'alta la derivació o l'ingrés i la data en què es realitza.

L'Entitat ha aportat el seu registre d'entrades i sortides de documents, fent-se constar el tipus de documentació, la data i hora, emissor/receptor, el número de documents, el tipus d'informació, la forma d'enviament i la persona responsable de la recepció o entrega degudament autoritzada.

Pel que fa als exàmens de salut laboral, durant els treballs de camp es constatà que l'entrega d'aquests quedaven registrats mitjançant un document que se'ls hi fa signar quan els treballadors reben l'examen per part del proveïdor que gestiona la prevenció de riscos laborals i vigilància de la salut.

Àrees de millora

▲	No detectada	

5.22. Fitxers temporals.

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

Situació actual

Durant els treballs de camp es constatà que és possible la generació de fitxers temporals, en el context de l'activitat diària de l'Entitat, encara que es té plena consciència de que, un cop finalitzada la tasca per la qual s'ha generat el document, aquest ha de ser destruït mitjançant la destructora de la que disposen a cada centre.

Així doncs, el punt 20 del Manual de Bones Pràctiques preveu que s'haurà de garantir el destí últim del paper inservible o duplicar mitjançant la seva destrucció a través de la màquina trituradora de paper o un servei extern especialitzat.

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 preveu l'existència en tots els DDSS d'un registre d'incidències que afecten a la seguretat de les dades tenint com a objectiu deixar constància dels problemes detectats en els fitxers de dades i de les actuacions derivades dels mateixos.

A més, l'Entitat disposa del document *Procediment de Gestió i Registre d'Incidències* per tal de notificar, gestionar i donar resposta a les incidències que es puguin produir i que afectin a la seguretat de les dades de l'Entitat.

Durant els treballs de camp es constatà que aquest registre d'incidències no és utilitzat pel diferent personal amb accés a dades de l'Entitat. Així doncs, el personal que detecta una incidència envia un correu electrònic al departament d'Administració i aquest informa al departament que correspongui segons el tipus d'incidència detectada.

L'Entitat tan sols ha aportat mostreig de les incidències detectades en l'àmbit informàtic però no les altres que puguin afectar a altres departaments de l'Entitat.

Àrees de millora

●	Àrea de millora	Cal que l'Entitat segueixi un únic procediment per la notificació, gestió i registre d'incidències que afecten a la seguretat de les dades. **Observació d'acord al nou RGPD:** Amb l'entrada en aplicació del RGPD a partir del 25 de maig de 2018, si es produeix una violació de la seguretat, el responsable l'ha de notificar a l'autoritat de control en un termini màxim de 72 hores, tret que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones. A més, quan sigui probable que la violació comporti un alt risc per als drets de les persones interessades, el responsable l'ha de comunicar a les persones afectades sense dilacions indegudes i en un llenguatge clar i senzill, tret que: – El responsable hagi adoptat mesures de protecció adequades, com ara que les dades no siguin intel·ligibles per a persones no autoritzades. – El responsable hagi aplicat mesures posteriors que garanteixen que ja no hi ha la probabilitat que es concreti l'alt risc. – Suposi un esforç desproporcionat.

5.24. Difusió de funcions i obligacions.

Base legal: Article 89.2 RD 1720/2007.

Situació actual

L'Entitat disposa d'un Manual de Bones Pràctiques en el qual consten les funcions i obligacions del personal, així com les conseqüències en cas d'incompliment d'aquestes funcions i obligacions.

Durant els treballs de camp, es constatà que el Manual de Bones Pràctiques és entregat a tots els treballadors de l'Entitat, així com un compromís de confidencialitat, havent-los de signar conforme s'ha realitzat l'entrega.

Pel que fa a la formació, durant els treballs de camps ens comentaren que tenen prevista fer una formació a tot el personal de cara al nou Reglament General de Protecció de Dades. També es comentà que les persones que s'encarreguen de la gestió de la protecció de dades assisteixen regularment a les formacions que s'organitzen des del Codi Tipus.

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.
5.5. Tercers. Prestacions sense accés a dades.
5.6. Legitimació de dades.
II- BLOC DE MESURES INFORMÀTIQUES
5.9. Connexions remotes
III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS
5.13. Registre d'accessos.
III – BLOC DE MESURES ORGANITZATIVES
5.23 Registre d'incidències

Barcelona, 16 de maig de 2018.

Pere Ruiz Espinós

- Soci-