**FUNDACIO PRIVADA INTERNACIONAL JOSEP CARRERAS**

# INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

*Número de Protocol 10.692*

## ÍNDEX

## 1. Objectius i contingut

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

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

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

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

## 2. Metodologia

Per portar a terme l'auditoria s'ha realitzat una revisió in situ de les instal·lacions de tractament de dades i sistemes d'informació de l'Entitat.

Tant la planificació, com el treball de camp d'auditoria, com també l'elaboració d'aquest informe han estat desenvolupats per un equip de persones constituït per professionals qualificats en el camp de la protecció de dades de *Faura-Casas, Auditors-Consultors SL* treballant de forma simultània els aspectes tècnics i organitzatius de la seguretat, així com 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 | Fundació Privada Internacional Josep Carreras |
| NIF | G-58734070 |
| Domicili | c/ Muntaner, 383<br><br>Barcelona - CP 08021 |

#### 3.1.2. Descripció de l'activitat

La Fundació fou constituïda el 1988 per escriptura del notari Juan José López-Burniol, número 3719 del seu protocol. En els seus estatuts s'identifica com a finalitat la lluita contra la leucèmia, investigació de noves tècniques per a combatre aquesta malaltia, aplicació de tecnologia en centres assistencials, assistència social als malalts i altres fins similars dins d'aquesta línia, tenint caràcter primordial tot el suport a la recerca i a l'assistència sanitària i clínica per a combatre el càncer i molt especialment, per a combatre la leucèmia.

Des de 1991 la Fundació gestiona, en estreta col·laboració amb el sistema de sanitat públic, *el registre oficial de donants de medul·la òssia a l'Estat espanyol*, REDMO.

La Fundació es finança, fonamentalment, gràcies a aportacions individuals o empresarials, a llegats, i als recitals i concerts benèfics de Josep Carreras. Tot l'esforç de la Fundació està dirigit a invertir aquests recursos a fer créixer l'esperança de les persones que pateixen leucèmia.

La informació es troba actualitzada en el web corporatiu http://www.fcarreras.org/ca

### 3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en el diversos departaments i àrees de la Fundació:

- Sistemes d'Informació
- Pacients
- Qualitat i Compliance
- Fidelització
- Actes Benèfics
- Comunicació i Màrqueting
- Donants
- SCU

També, s'han visualitzat les zones compartides, d'accés i custòdia de documentació.

### 3.2.1. Data de realització de l'auditoria

| | |
|---|---|
| **Dia** | 11 i 12 de desembre 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** | Mavi Díaz Morales | Pacients |
| **2** | Núria Marieges | Coordinació REDMO |
| **3** | Mario Gran | Sistemes d'Informació |
| **4** | Jordi Llobet | Informàtic extern – EPI |
| **5** | Anna Giner | Gestió i Qualitat |
| **6** | Laura Lorenzo | Fidelització |
| **7** | Regina Díez | Actes Benèfics |
| **8** | Albertina Grau | Socis, actes benèfics i herències |
| **9** | Alexandra Carpentier de Changy | Premsa, Comunicació i E-Màrqueting |
| **10** | Marta Fernández | Premsa, Comunicació i E-Màrqueting |
| **11** | Núria Giménez | Departament de donants |
| **12** | Cristina Bueno | Departament de donants |
| **13** | Montserrat Rebagliato | Departament de Sang de Cordó Umbilical |

Relació de la documentació lliurada a l'auditor:

| **Documents** |
|---|
| Escriptura de constitució i Organigrama |
| Document de Seguretat |
| Cartes notificacions fitxers Agencia Española de Protección de Datos |

| |
|---|
| Informes de les auditories de protecció de dades de 2013 i 2015 |
| Contractes i convenis amb tercers |
| Protocols de circulars interns |
| Descripció de xarxa i altre detall de recursos informàtics |
| Clàusules en diferents documents de legitimació (imatges, actes benèfics, etc.) |
| Ordre del dia de l'última Junta de patronat |
| Clàusules formularis web |

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

La Fundació Internacional Josep Carreras, en endavant la Fundació o l'Entitat, va realitzar la darrera auditoria en matèria de protecció de dades el desembre de 2015, complint amb les previsions legalment establertes en l'article 96 del RDLOPD, segons el que es preveu el criteri de biennalitat en la realització d'auditories.

En la Junta de patronat de 20 d'abril de 2017 apareix en el punt 15.4 de l'ordre del dia *"Inf. Compliment legislació protecció de dades"*, a través del qual es pot confirmar que es fa el seguiment de l'última auditoria per part del responsable del fitxer.

### Àrees de millora

| | | |
|---|---|---|
| ? | No detectada | Cal que l'informe d'auditoria no només sigui analitzat pel responsable de seguretat competent, sinó que siguin elevades les conclusions al responsable del fitxer de manera documentada de manera que n'adopti les mesures correctores adequades i tot plegat quedi a disposició de l'Agencia Española de Protección de Datos (AEPD). |

### 5.2. Aspectes generals.

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

**Situació actual**

L'entitat ha fet entrega de les cartes de tramitació de diversos fitxers a l'Agencia Española de Protección de Datos. No obstant, si es fa la consulta en el registre de l'AEPD, es comprova que (sota un mateix NIF) l'Entitat té notificats 8 fitxers a data actual sota 3 diferents noms: *Fundación Internacional José Carreras para la Lucha contra la Leucemia*, *Fundación Internacional Josep Carreras* i *Fundación Internacional Josep Carreras para la Lucha Contra la Leucemia*. Malgrat ser un error menor, convé modificar-ho i harmonitzar la denominació del responsable del fitxer a la que sigui la denominació oficial de l'Entitat.

A continuació s'indiquen els fitxers que figuren en el registre amb detall dels diferents camps:

| FITXER | CODI | FINALITAT | NIVELL | TRACTAMENT |
|---|---|---|---|---|
| REDMO | 1942245789 | *EL FICHERO CONTIENE INFORMACION SOBRE LAS CARACTERISTICAS GENETICAS SOBRE LOS DONANTES PARA PODER DETERMINAR LA COMPATIBILIDAD DE LOS MISMOSCON PACIENTES CANDIDATOS A UN TRASPLANTE DE MEDULA OSEA* | Alt | Automatitzat |
| DONANTS | 1960190024 | *GESTIÓN Y MANTENIMIENTO DE LOS DONANTES ECONÓMICOS DE LA FUNDACIÓN INTERNACIONAL JOSEP CARRERAS DONANTES CON APORTACIONES PERIÓDICAS O PUNTUALES* | Alt | Automatitzat |

| | | | | |
|---|---|---|---|---|
| POSSIBLES | 2060240260 | *GESTIÓN Y MANTENIMIENTO DE LAS PERSONAS QUE SOLICITAN INFORMACIÓN O ESTÁN INTERESADOS EN LA LABOR DE LA FUNDACIÓN INTERNACIONAL JOSEP CARRERAS ASÍ COMO LA REALIZACIÓN DE ACTIVIDADES CON IMPACTO MEDIÁTICO Y/O COMERCIAL PARA PROMOCIONAR LA FUNDACIÓN INTERNACIONAL JOSEP CARRERAS* | Alt | Automatitzat |
| FIJC | 2023470076 | *GESTION CONTABLE* | Bàsic | Automatitzat |
| FORUM | 2101191373 | *FICHERO DONDE SE GUARDAN TODOS LOS E MAILS DE LOS USUARIOS QUE SE REGISTRAN EN EL FORUM DE LA PAGINA WEB DE LA FUNDACION INTERNACIONAL JOSEP CARRERAS* | Bàsic | Mixt |
| NEWSLETTER | 2141741633 | *COMUNICACION VIA CORREO ELECTRONICO DE LAS NOTICIAS DE LA FUNDACION INTERNACIONAL JOSEP CARRERAS Y DEL INSTITUTO DE INVESTIGACION CONTRA LA LEUCEMIA JOSEP CARRERAS AL PERSONAL DE AMBOS Y A PERSONAS QUE COLABORAN ESTRECHAMENTE CON ELLOS COMO SON HOSPITALES FACULTADES GENERALITAT* | Bàsic | Automatitzat |
| NOMINA | 1942534821 | *ELABORACION DE LA NOMINA Y COTIZACIONES A LA SS DE LA COMPAÑIA Y GESTION DE LOS RECURSOS HUMANOS ELABORACIONES DE ESTADISTICAS DE USO INTERNO* | Bàsic | Automatitzat |

| | | | | |
|---|---|---|---|---|
| NOMINA EXTERNO | 2060240276 | *CONFECCION DE LAS NOMINAS Y SEGUROS SOCIALES DE LOS TRABAJADORES DE LA FUNDACION JOSEP CARRERAS* | Alt | Automatitzat |
| RECEPTOR | 2030270031 | *REALIZAR BUSQUEDAS DE COMPATIBILIDAD PARA PACIENTES EN ESPERA DE TRASPLANTE DE MEDULA OSEA* | Alt | Automatitzat |

## Àrees de millora

| | | |
|---|---|---|
| ? | No detectada | Convé que l'Entitat unifiqui la seva denominació com a responsable dels diferents fitxers que consten al registre de l'AEPD.<br><br>En tant que fundació, és recomanable notificar un fitxer en relació amb el blanqueig, en virtut del que disposa la Llei 10/2010, de 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme.<br><br>Es suggereix valorar la re configuració dels fitxers actuals i re definir-la segons finalitats que puguin derivar d'un únic fitxer. A mode d'exemple, es proposa el següent: Nomina i Noma Extern en un de sol dit *Personal*, Newsletter, Possibles i Forum en un de sol dit *Activitat*, Redmo i Receptors en un de sol dit *Pacients*. També, dir que el fitxer *Donants* pot donar peu a confusió, doncs es refereix a socis i no pas a persones donants d'òrgan o teixit, motiu pel qual fóra convenient modificar-ne la nomenclatura. |

### 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:<br>• L'entitat ha elaborat un únic DS que inclou tots els fitxers dels quals és responsable.<br>• El DS aportat sembla que estigui en versió esborrany, doncs en aquest hi apareixen marques i punts pendents de desenvolupar, per exemple en l'Annex I Registre d'Usuaris.<br>• El DS no conté cap signatura ni es fa evident que s'hagi aprovat per la persona responsable, tampoc hi figura cap data d'elaboració ni revisió, o versió del mateix amb canvis inclosos.<br>• Tampoc hi ha evidència que aquest document hagi estat difós a tot el personal i/o explicat degudament. |
| **B.** Àmbit d'aplicació del document amb especificació detallada dels recursos protegits:<br>o Inventari de suports.<br>o Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten. |
| Comentaris:<br>• S'identifica en el punt 1 del DS l'àmbit d'aplicació i en el punt 2 del mateix quins són els recursos protegits. |

- Consta el detall dels fitxers als quals es fa referència.

- Es descriuen els sistemes d'informació que s'utilitzen per als tractaments dels fitxers.

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

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

Comentari:

- No s'inclou cap descripció sobre aquest punt.

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

Comentaris:

- En el punt 3 del DS s'hi descriuen les mesures, normes, procediments i regles que garanteixen el nivell de seguretat.
- També, en el punt 4 del DS trobem la descripció dels sistemes d'informació que tracten els fitxers amb dades de caràcter personal.

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

Comentaris:

- Es descriu en el punt 6 del DS, Funcions i Obligacions del Personal.
- També, en el punt 8 del DS es relacionen les mesures preses per tal que el personal conegui les normes de seguretat.
- També, en l'Annex 3 del DS s'incorpora una informació bàsica adreçada a tot usuari de fitxers amb dades de caràcter personal.

| |
|---|
| **F.** Procediment de notificació, gestió i resposta davant les incidències. |
| Comentaris:<br>• Queda descrit en el punt 5 del DS, Procediment de notificació, gestió i resposta davant d'incidències, i Annex 2 del mateix, sota el títol de registre d'Incidències. |
| **G.** Procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats. |
| Comentaris:<br>• Queda descrit dins del punt 3 del DS en un subapartat específic relatiu a còpies de seguretat. |
| **H.** Mesures que sigui necessari adoptar per al transport de suports i documents, així com per a la destrucció dels documents i suports o, si s'escau, la reutilització d'aquests últims. |
| Comentaris:<br>• El DS no conté cap descripció específica d'aquest punt. |
| **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 si el tractament es realitza, o no, en els locals del responsable. |
| Comentari:<br>• No queda especificat en el DS aquest punt. |
| **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:<br><br>• No consta que l'Entitat actuï en cap cas com a encarregada de tractament. |
| **Autoritzacions** |
| **K.** Autorització per a l'emmagatzematge de dades de caràcter personal en dispositius portàtils (usuaris/ perfils d'usuaris i període de validesa).<br><br>Tractament de dades de caràcter personal en dispositius portàtils que no permetin el xifratge. |
| Comentaris:<br><br>• No es regula de forma específica, només es fa algun apunt sobre aquesta qüestió dins de l'Annex 3. |
| **L.** En relació al tractament de dades de caràcter personal fora dels locals del responsable, cal que hi hagi l'autorització així com els usuaris/ perfils d'usuaris i el període de validesa per a aquest tractament. |
| Comentari:<br><br>• No es fa constar al DS les connexions que es realitzen fora dels locals del responsable ni per part del personal, ni tampoc per part de proveïdors externs. Únicament dins del punt de Seguretat Lògica, es menciona que la persona amb condició d'administrador (responsable de SSII de l'Entitat o informàtics de l'empresa EPI) poden accedir en remot, punt a punt o presencial. |
| **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:<br><br>• El DS no especifica dins del punt de la gestió d'usuaris qui és el personal autoritzat per concedir, alterar o anul·lar l'accés autoritzat sobre els recursos. |

| |
|---|
| **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:<br>• No hi ha cap referència concreta a l'accessibilitat als equips i espais físics. |
| **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:<br>• No es fa una descripció concreta sobre aquest punt en el DS. |
| **P.** Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic. |
| Comentari:<br>• En el DS es descriu el correu electrònic a través de l'Exchange Online, també el Docuware per la gestió documental. Ara bé, no hi consten indicacions específiques com requereix la norma. |
| **Q.** Personal autoritzat per a la recepció/ enviament de dades de caràcter personal *(nivell mitjà i/ o alt)*. |
| Comentari:<br>• No hi ha cap descripció concreta d'aquest punt en el DS. |
| **R.** Personal autoritzat per a la realització del procediment de recuperació de dades. |
| Comentari:<br>• No hi ha cap descripció específica sobre aquest punt, només es fa una simple menció dins de l'Annex 3. |

| |
|---|
| **S.** Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen. |
| Comentari:<br><br>• No consta en el DS una relació de persones a qui s'hagin delegat autoritzacions per part del responsable del fitxer. |
| **Altres mesures** |
| **T.** Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat. |
| Comentaris:<br><br>• No es descriu com a punt del DS, tot i que s'hi fa esment dins de l'apartat VI de la Gestió d'Usuaris.<br>• En l'Annex 3 es fa una previsió de compartir bústies personals entre usuaris, la qual cosa no seria ajustada a la normativa. |
| **U.** Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions. |
| Comentari:<br><br>• No queda estipulat en el DS el període de canvi de contrasenyes en l'accés al sistema o aplicacions. |
| **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:<br><br>• No consta cap menció al respecte dins del DS. |
| **W.** Identificació del responsable de seguretat *(nivell mitjà i/ o alt).* |

| |
|---|
| Comentari:<br><br>• No s'identifica la figura del responsable de seguretat en el DS. |
| **X.** Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt)*. |
| Comentari:<br><br>• El punt 9 del DS fa referència als controls periòdics per a verificar el compliment del DS |

## Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Cal actualitzar el DS amb els aspectes que s'indiquen pendents de desenvolupar. A més, recordar que el DS és un document dinàmic que ha de respondre a la realitat de l'Entitat, per la qual cosa convé revisar-lo periòdicament.<br><br>El DS ha de ser validat pel responsable del fitxer i així ha de constar.<br><br>L'Entitat pot aprofitar l'existència de protocols de seguretat, confidencialitat o bona praxi per annexar-los en el DS. |

### 5.4. Delegació d'autoritzacions.

***Base legal: Article 84 RD 1720/2007.***

## Situació actual

D'acord amb l'anterior punt 5.3.S d'aquest informe, no consta cap delegació de funcions a dia d'avui.

En cas que el responsable del fitxer hagi encomanat a alguna persona tasques concretes és necessari que quedi descrit dins del DS, identificant quines són aquestes delegacions i autoritzacions, així com també els circuits de control que sobre les mateixes puguin establir-se.

## Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de millora | Cal que l'Entitat en determini i faci constar documentalment les delegacions i autoritzacions als Documents de Seguretat per tal de tenir controlats tots els circuits i protocols.<br><br>Fóra molt recomanable que hi hagi a més dels corresponents responsables de seguretat, també un conjunt de persones que de forma periòdica revisessin els aspectes relatius a protecció de dades, a mode de comissió o grup de treball, per tal que pugui estar-se permanentment informat de qualsevol canvi i/o incidència en aquesta matèria que es produeixi. |

### 5.5. Tercers.

### ENCARREGATS DE TRACTAMENT

***Base legal: Article 82 RD 1720/2007.***

**Situació actual**

Com s'ha comentat al punt 5.3.I, el DS no recull un llistat d'Encarregats del Tractament on s'especifiqui el nom de les entitats, la descripció del servei prestat, el fitxer al qual accedeixen, el tipus de contracte, vigència, localització del tractament.... No obstant això, l'Entitat aporta els contractes que es valoren a continuació:

| ET's ANALITZATS | SERVEI PRESTAT | CONTRACTE | COMENTARIS |
|---|---|---|---|
| **CASA ROJALS SL** | Custòdia documental | ☒ | El document d'11 d'octubre de 2016 no s'ajusta a les estipulacions de l'article 12 de la LOPD. |
| **ZOHAR i DATEM** | Accions de telemàrqueting | ☑ | En el contracte de 10 de març de 2016 no s'estableixen les mesures de seguretat requerides. |
| **Estudi i Projectes Informàtics** | Serveis informàtics | ☑ | En el contracte de 9 de maig de 2012 no s'estableixen les mesures de seguretat requerides. |
| **Associació Catalana d'Esclerosis Múltiple** | Suport en accions de devolució de correu postal i trucades | ☑ | En el contracte de 14 d'abril de 2014 no s'estableixen les mesures de seguretat requerides, a més de citar-se normativa derogada. |
| **NTI Figueras SL** | Enviament documentació | ☑ | En el contracte de 31 de març de 2016 no s'estableixen les mesures de seguretat requerides, a més de citar-se normativa derogada. |
| **WESSER & PARTNER SL** | Captació de socis | ☑ | En el contracte d'1 de gener de 2008 no s'estableixen les mesures de seguretat requerides. |

## Salvetat

| | | |
|---|---|---|
| ? | Salvetat | Cal que l'Entitat signi amb els proveïdors que tinguin accés a dades els corresponents contractes d'encarregat del tractament.<br><br>Per altra banda, pel que fa al llistat de proveïdors, cal que s'especifiqui si es tracta d'encarregats del tractament o bé prestador de servei sense accés a dades. Aquest llistat, per altra banda, haurà de complir amb allò que s'especificà al punt 5.3.1 del present informe.<br><br>També, convé revisar i harmonitzar els acords derivats del REDMO entre l'Entitat i les diferents Comunitats Autònomes. |

### PRESTACIONS SENSE ACCÉS A DADES

***Base legal: Article 83 RD 1720/2007.***

## Situació actual

Per part de l'Entitat s'ha facilitat un únic proveïdor, el qual és analitzat a continuació:

| TERCERS SENSE ACCÉS | SERVEI PRESTAT | COMPROMÍS | COMENTARIS |
|---|---|---|---|
| **ECOLOGIC** | Gestió residus documentals | ☒ | S'aporta certificat de 21 de desembre de 2016 en el qual no hi consten els requeriments de l'article 83 del RLOPD. |

## Salvetat

| | | |
|---|---|---|
| ? | Salvetat | Cal que l'Entitat signi un contracte en el qual s'incloguin els aspectes de l'article 83 del RLOPD, és a dir, reculli expressament la prohibició d'accedir a les dades personals i l'obligació de secret respecte a les dades que el personal hagués pogut conèixer amb motiu de la prestació del servei.<br><br>Per altra banda, pel que fa al llistat de proveïdors, cal que s'especifiqui si es tracta d'encarregats del tractament o bé prestador de servei sense accés a dades. |

### 5.6. Legitimació de dades.

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

**Situació actual**

S'analitza a continuació on s'evidencia la legitimació de les dades, segons els formularis que s'han facilitat, dels fitxers de l'entitat:

| FITXER | LEGITIMACIÓ | COMENTARIS |
|---|---|---|
| **REDMO** | Els diferents hospitals proveeixen les dades de les persones que consten en el registre. En aquest hi apareixen les persones donants. | La legitimació de les dades correspon als centres als quals la persona formalitza la seva condició de donant. No obstant, en la carta de benvinguda que s'emet des de la Fundació hauria d'incloure's una clàusula informativa de protecció de dades en els termes de l'article 5 LOPD. |
| **NOMINA**<br><br>**NOMINA EXTERN** | Existeix un document pel qual s'informa a tot treballador respecte a la cura que ha de tenir en el tractament de dades personals. No obstant, en cap cas s'informa al treballador de l'ús de les seves dades que farà l'Entitat. | Cal que l'Entitat inclogui una clàusula informativa en els termes de l'article 5 LOPD per tal de legitimar el tractament de les dades dels treballadors en base amb la relació laboral. |

| | | |
|---|---|---|
| **POSSIBLES**<br><br>**FORUM**<br><br>**NEWSLETTER** | Existeixen vàries informacions relacionades amb la protecció de dades al voltant dels col·lectius de "Possibles" o "Amics", les quals no acompleixen totalment amb la normativa de protecció de dades.<br><br>El newsletter conté una informació bàsica però no suficient en termes de protecció de dades. | Caldria redactar una nova clàusula informativa que s'inclogués en el newsletter.<br><br>Així mateix, totes les accions que l'Entitat vulgui fer amb persones no sòcies han d'anar precedides per una informació en els termes de l'article 5 LOPD. |
| **RECEPTOR** | No consta legitimació de dades sobre aquest fitxer | Cal informar al receptor de medul·la òssia del contingut de l'article 5 LOPD en relació a aquest fitxer. |
| **DONANTS** | S'aporta el formulari en el qual es recullen les dades del donant/soci.<br><br>El formulari d'actes benèfics incorpora una clàusula de protecció de dades. | La clàusula informativa no s'ajusta a les especificacions de l'article 5 LOPD en relació amb aquest fitxer.<br><br>La clàusula informativa és incompleta respecte als requeriments de l'article 5 LOPD. |
| **FIJC** | No consta legitimació de dades sobre aquest fitxer | Cal informar, quan els clients o els usuaris siguin persones físiques, sobre les especificacions de l'article 5 de la LOPD en relació a aquest fitxer. |

A banda de les legitimacions dels fitxers declarats, també s'observen altres tractaments de dades que no quedarien a dia d'avui inclosos dins dels dits fitxers però que es fa necessari comentar. En primer lloc, en l'activitat de l'Entitat també es gestionen pisos de famílies i a aquest efecte, es formalitza el degut contracte de pis d'acollida en el qual no hi consta cap clàusula sobre protecció de dades. En segon lloc, són varis els departaments que

utilitzen documents d'autorització d'imatges /vídeos, en tots ells cal modificar la clàusula informativa de protecció de dades. En tercer lloc, s'ha de revisar la política de privacitat del web corporatiu de l'Entitat i adequar el contingut en protecció de dades, així com també incloure a La Botiga Online.

## Àrees de millora

| | | |
|---|---|---|
| ? | Salvetat | L'Entitat haurà de modificar les clàusules informatives actuals per tal que puguin ajustar-se als requeriments de l'article 5 LOPD, així com també als fitxers dels quals l'Entitat és responsable. |

### 5.7. Drets ARCO.

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

## Situació actual

Tal i com s'exposava en anteriorment, el document de seguretat no fa referència als drets ARCO, tampoc existeixen com a Annexos models dels formularis a emplenar o bé circuit a seguir en cas d'eventuals exercicis de drets, la qual cosa és necessària. Tampoc existeix de facto cap persona de l'organització a qui es centralitzi aquesta qüestió.

Durant l'auditoria es posà de manifest que no hi ha constància d'haver rebut cap petició de dret ARCO en aquests termes. No obstant això, es fa notar que periòdicament sí que es produeixen sol·licituds de rectificació de dades (per part de persones sòcies de l'Entitat), o bé baixes (també per part de persones sòcies, per motius econòmics fonamentalment). Davant d'aquests casos, s'actua seguint la petició rebuda, és a dir, es procedeix a la modificació de les dades com s'indica, o bé s'anota en el programa l'ordre de baixa de soci per eliminar el deure de pagament. Malgrat això, s'observa que en els casos en què es demana baixa, no es produeix una baixa en sentit rigorós, doncs a la persona que deixa de col·laborar econòmicament se li segueixen fent comunicats i/o enviaments, la qual cosa no s'ajustaria als requeriments normatius.

Dir també que en totes les clàusules informatives de protecció de dades caldrà revisar el punt relatiu als drets ARCO, a efectes de confirmar l'adreça a on dirigir-los i/o persona/unitat responsable.

## Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Cal que l'Entitat descrigui el protocol relatiu a drets ARCO, dissenyi el circuit d'atenció a aquests drets i els doni resposta dins de termini.<br><br>S'haurà d'explicar el significat i abast de cadascun dels drets per tal que no es contravinguin les previsions legals, sobretot pel què fa al dret de cancel·lació de dades, que pot produir importants conseqüències d'infracció si no s'aplica correctament. |

## II - BLOC DE MESURES INFORMÀTIQUES

### 5.8. Accés a xarxes.

***Base legal: Article 85 RD 1720/2007.***

**Situació actual**

Com s'ha comentat al punt 5.3.B del present informe, l'Entitat recull en el document de seguretat el detall dels recursos protegits i la identificació de les mesures que garanteixen el nivell de seguretat. Paral·lelament al document de seguretat, hi ha constància d'altres protocols relatius a la seguretat informàtica (SD-001 gràfic de sistemes, SD-001 Data Sheet Endpoint Security, PRD Microsoft Azure, etc.), els quals fóra convenient adjuntar com a annexos al propi DS.

Segons aquests documents, es fa esment a 2 tipus de sistemes d'antivirus, un per als servidors i un altre per a les estacions de treball. El del servidor és un Microsoft Windows Defender, mentre que el de les estacions de treball és Symantec Endpoint Protection versió 14.

La infraestructura informàtica de TI de l'organització es troba en un entorn híbrid de núvol privat sobre servidors locals a les dependències de la Fundació 9i una infraestructura allotjada en núvol públic de Microsoft Axure. Aquests 2 entorns es comuniquen a través de diferents sistemes: en alguns casos, s'utilitzen agents que estableixen comunicacions directes via internet, altres serveis utilitzen una VPN per a connexions entre núvol públic, núvol privat i xarxa local.

Es disposa de 24 servidors amb Windows Server 2012 R2 i Windows Server 2016 i 31 estacions de treball amb Windows 7, 8.1 i 10.

Les comunicacions amb internet es realitzen via connexions redundants amb diferents tecnologies i s'utilitzen firewall per hardware instal·lat en els servidors de Hyper-V i internet. En aquests moments, es disposa de dues connexions a internet amb tecnologies diferents: fibra i 4G, així com també proveïdors diferents que garanteixen el servei permanent. Ambdós sistemes tenen ADSL de suport.

El núvol privat (local) està implementat sobre varis servidors Microsoft Windows Server 2016 Hyper-V i executen màquines virtuals, duent a terme serveis a:

- Servidors de domini Microsoft Active Directory
- Servidors de bases de dades Microsoft SQL 2016
- Servidors de Business Intelligence
- Servidors de fitxers. Servei DFS
- Servidors d'aplicacions (Epidonor)
- Servidors d'aplicacions de comunicació
- Altres servidors per a desenvolupament, integració d'aplicacions, etc.

Els servidors Hyper-V tenen ubicació d'accés físic restringit, amb doble aire condicionat, sistema d'alarma de foc i temperatura i sistema SAI. Tots aquests servidors tenen equips de xarxa i utilitzen VLAN per a beneficiar a tots els servidors virtuals implementats i totes les seves comunicacions de xarxa.

D'altra banda, s'utilitzen serveis de Microsoft Office 365 per a tot el sistema de correu electrònic, col·laboració, emmagatzematge i compartició de fitxers, comunicacions, gestió de calendaris i gestió de contactes. També, per a serveis de còpies de seguretat, anàlisis de dades amb Business Intelligence, recuperació de desastres, allotjament d'aplicacions i serveis de bases de dades. Els dits serveis s'integren en el directori actiu local de forma que es comparteix autenticació, autorització i seguretat d'usuari, grups i permisos d'aplicacions.

## Àrees de millora

| | | |
|---|---|---|
| ? | No detectada | *Veure punt 5.3.B de l'informe.* |

### 5.9. Connexions remotes.

***Base legal: Article 86 RD 1720/2007.***

## Situació actual

Tal com s'ha comentat al punt 5.3.L, l'Entitat no fa constar al DS les connexions realitzades fora dels locals del responsable, si bé es descriuen mesures de seguretat sobre les dades i aplicacions que les gestionen, que operen tant a mode local com remot.

Tots els usuaris s'identifiquen a través de l'actiu directori, des d'on es gestionen els permisos. Tanmateix, no existeix cap circuit que defineixi el circuit que s'ha de realitzar per gestionar les baixes d'aquests permisos, tot i que la contrasenya en caduca.

## Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de Millora | Cal que l'Entitat, en virtut de l'article 86 del RLOPD inclogui a tots els usuaris interns, o externs (entenent-se usuari com treballador, autònom o empresa) que accedeixen remotament dins del DS.<br><br>Caldrà, per altra banda, protocol·litzar les baixes de la vigència per a connectar-se remotament per tal d'evitar-ne accessos indeguts.<br><br>*Tenir en compte el punt 5.3.L* |

### 5.10. Transmissions per xarxes de telecomunicacions.

***Base legal: Article 104 RD 1720/2007.***

#### Situació actual

Malgrat la descripció de les mesures de seguretat que es contempla en el document de seguretat, durant els treballs de camp es detectà que és habitual que es facin enviaments amb informació sensible per correu electrònic sense xifrar, així com puntualment també per fax. Aquests mecanismes no s'ajusten als requeriments de seguretat definits per la norma, de manera que caldria reconduir-los a d'altres que permetin les comunicacions amb seguretat.

D'altra banda, fer esment que existeixen vàries fonts que proveeixen d'informació a la Fundació. Aquesta informació és comunicada sempre per canals encriptats i segurs:

- EMDIS – els correus electrònics estan encriptats i firmats amb l'eina de xifrat i firmes digitals GnuPG versió 2.0.30 (PGP)
- Aplicació web d'entrada o modificació de donants (EPICdp i Episocis Proveïdors) – s'utilitza el certificat SSL amb clau 256 bits que garanteix que el lloc és autèntic, real i confiable per ingressar les dades personals. La comunicació entre el servidor i l'usuari es fa totalment xifrada. Els certificats són renovats periòdicament i atorgats per Thawte.

#### Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Cal que la Fundació defineixi noves vies d'enviament de la informació a través de mètodes que garanteixin totes les mesures de seguretat, no essent adequats ni el fax ni el correu electrònic sense xifrar. |

### 5.11. Control d'accés.

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

## Situació actual

Tots els usuaris amb accés als recursos de la Fundació es troben en el directori actiu, on s'hi pot visualitzar si l'usuari és alta o baixa, així com els diferents permisos atorgats.

Es descriu la gestió d'usuaris en el document de seguretat. La gestió de permisos i polítiques es controla pel responsable IT. Els permisos d'accés a la informació ofereixen mode lectura o edició, accés a opcions, pestanyes, segons permisos atorgats.

Durant els treballs de camp, es detectà que si bé en el moment d'una nova incorporació el procediment és molt rigorós (els drets d'accés són configurats pel personal IT i determinats per gerència), no és tant així en casos en què es puguin produir certes baixes. Caldria en tot cas, tenir evidència que qualsevol persona que té accés als recursos estigui degudament autoritzada, en virtut de l'exercici de les tasques que té encomanades.

Així mateix, es constatà que gran part dels treballadors tenen accessos per defecte o privilegis que el seu lloc de treball no justificaria, la qual cosa fa pertinent la revisió de l'assignació de permisos per usuaris amb la intenció de que no es disposi d'accés a eines o informació que no es requereix per la seva feina.

En el document de seguretat hi consta com a Annex I el *Registre d'Usuaris*, el qual identifica els següents camps: Nom_DNI_Alta_Baixa_Departament_Accés de dades autoritzat/Fitxers.

## Àrees de millora

| | | |
|---|---|---|
| ▼ | Salvetat | Cal que l'Entitat tingui protocol·litzat en el document de seguretat el procediment d'altes i baixes dels usuaris als diferents programaris i, per altra banda, es defineixin els usuaris o perfils que tenen accés a cada fitxer, atenent a les seves funcions. |

### 5.12. Identificació i autenticació d'usuaris.

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

## Situació actual

Tot el personal amb accés al sistema i als programes disposa d'usuari i contrasenya, de manera que es garanteix la correcta identificació i autenticació dels usuaris. La identificació de qualsevol usuari per accedir al sistema i als programes és inequívoca i personalitzada. Aquesta es descriu en part dins del punt de Gestió d'Usuaris del document de seguretat, segons el qual l'accés de tot usuari ha de ser a través de nom d'usuari i contrasenya. Existeix una política de contrasenyes segura que inclou una longitud mínima, una complexitat amb ús d'almenys majúscules, minúscules, números, lletres i/o signes, etc. la política contempla la caducitat cada 6 mesos, així com un històric de contrasenyes per evitar repeticions. La validació en el sistema és la mateixa que permet l'accés als programes en els quals l'usuari té permisos assignats, s'utilitzen les polítiques de Microsoft Active Directory per confirmar l'usuari.

Malgrat que en l'Annex 3 s'imposa el deure de "no proporcionar l'identificador de l'usuari a tercers ni claus d'accés", durant els treballs de camp es confirmà que en determinades unitats diferents usuaris coneixien les contrasenyes personals d'altres companys, la qual cosa vulneraria la norma.

En aquests moments no es disposa d'un single sign on que permeti una única validació de l'usuari al sistema i diversos programaris que s'utilitzen, si bé a través de la contrasenya de Microsoft es lliga automàticament l'accessibilitat de l'usuari als aplicatius.

Existeix bloqueig davant de 50 intents reiterats no autoritzats. Si bé aquesta mesura no és incorrecte, es recomana per motius de seguretat que es baixi el nombre d'intents.

Per últim, l'Entitat emmagatzema les contrasenyes de forma inintel·ligible i, en cas d'incidència o pèrdua, el responsable d'informàtica només pot establir-ne una de nova. Aquest procediment garanteix la seva confidencialitat i integritat.

## Àrees de millora

| | | |
|---|---|---|
| ▼ | Salvetat | *Els usuaris exclusivament han de tenir accés als recursos necessaris per a l'exercici de les seves funcions.*<br><br>*Els accessos han de ser individualitzats de manera que es permeti la màxima traçabilitat de les accions de cada usuari, en cas d'haver de compartir informació, caldria disposar de comptes compartides o accessos que no es lliguin a un identificador personal.* |

### 5.13. Registre d'accessos.

***Base legal: Article 103 RD 1720/2007.***

## Situació actual

Aquesta mesura només seria exigible als fitxers automatitzats de nivell alt que gestiona la Fundació, és a dir: Receptors, REDMO, Donants i Possibles.

No queda descrit ni en el document de seguretat ni tampoc en cap annex al mateix que l'Entitat apliqui les pautes de traçabilitat requerides. No obstant això, s'informa que ...*"els sistemes d'informació contemplen l'ús de monitorització i auditoria de la informació i de les aplicacions. En alguns casos s'auditen les modificacions a nivell de registre i camp per a determinats orígens, podent conèixer qui ha modificat una dada, quan i des d'on"*. Es manifesta que els canvis queden conservats dins de les taules del propi SQL amb caràcter indefinit.

Respecte a la revisió que s'efectua del dit registre d'accessos, malgrat que els diferents programes tenen incorporat un mòdul per controlar els accessos i detectar-ne els accessos indeguts, tanmateix no consta que s'estigui fent mensualment una revisió d'aquesta informació enregistrada, així com tampoc s'elabora l'informe de la dita revisió en els termes en què obliga la norma.

## Salvetat

| | | |
|---|---|---|
| ? | Salvetat | El Responsable de Seguretat o persona delegada cal que revisi mensualment i elabori els preceptius informes de revisió mensual de cadascuna de les aplicacions amb dades de nivell alt, en el que hi consti una revisió dels accessos esdevinguts i dels problemes detectats.<br><br>Recordar a l'Entitat que la informació emmagatzemada derivat de la traçabilitat haurà de ser custodiada durant un període de 2 anys. |

### 5.14. Còpies de seguretat.

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

## Situació actual

D'acord allò que s'ha comentat al punt 5.3.G del present informe, el DS fa esment a les còpies de seguretat. Segons aquest, per al núvol privat (local) existeix un servidor de còpies de seguretat (DPM) que centralitza i gestiona tot el sistema de còpies de seguretat i restauracions de la Fundació. En efecte, el DPM realitza còpies de seguretat dels fitxers allotjats en el servidor DFS i de les bases de dades SQL.

Les còpies de seguretat tenen una periodicitat que va des de cada 15 minuts per a les bases de dades fins a un mínim d'una còpia diària.

Les còpies es realitzen en un sistema de discos en el DPM local per a recuperacions ràpides i a més, es realitzen còpies al núvol de Microsoft Azure per a garantir una còpia en un lloc segur i extern a l'Entitat.

Les retencions de les còpies varien des de retencions de totes les còpies diàries durant un mes a retencions de còpies anuals fins a 10 o 20 anys. Existeixen polítiques de retencions diàries, setmanals, mensuals i anuals. El sistema permet la recuperació de gran quantitat de punts de recuperació.

Respecte a les còpies del núvol públic de Microsoft Azure, situades fora de la Fundació, tenen directives de retenció de 180 dies, de 104 setmanes, 60 mesos i 15 anys augmentables a més de 20 anys.

Existeix un sistema preparat per a permetre la recuperació en cas de pèrdua parcial del núvol privat, inclòs el servidor DPM. Una màquina virtual de reserva permet la recuperació de qualsevol còpia en Azure de manera àgil i el més ràpida possible.

En cas de desastre que inclogués la pèrdua de tot el núvol privat i servidors locals també és possible la recuperació des del núvol públic Microsoft Azure de les còpies de seguretat. Aquestes còpies garanteixen una rèplica geogràfica de còpies de seguretat i un acord de nivell de servei (SLA) del 99,99%.

Pel que fa a les verificacions d'aquestes còpies, l'Entitat afirma que es realitzen, si bé no queda documentat.

## Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de millora | *Cal que l'Entitat tingui evidència de verificar el sistema de còpies de seguretat com a mínim amb periodicitat semestral.* |

### 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 que es produeixin aquest tipus de documents. Tanmateix, durant l'auditoria es constatà que els usuaris treballaven sobre els programaris específics o bé des de carpetes que es troben ubicades a la xarxa, dins del servidor. No es detectà que els usuaris disposessin d'arxius en la unitat local o en altres espais fora de control.

Addicionalment, com s'ha anat apuntant, cal afegir que tot i que les sortides dels ports USB es troben obertes, no queda cap tipus d'informació emmagatzemada dins dels discs durs dels equips, donat que aquesta sempre s'allotja a la xarxa.

No obstant l'anterior, es manifestà que la informació continguda dins de les carpetes de la xarxa no és eliminada un cop transcorreguda la seva finalitat. Per aquest motiu, es va avinent que es procedeixi a la revisió i supressió d'aquells documents que no tenen utilitat i/o que es troben duplicats.

## Àrees de millora

| | | |
|---|---|---|
| ? | No detectada | *Cal que es facin recomanacions per tal de conscienciar als treballadors en relació amb els fitxers temporals.* |

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

***Base legal: Article 97 RD 1720/ 2007.***

## Situació actual

En el document de seguretat no es fa cap previsió sobre el registre d'entrades i sortides de suports. Durant els treballs de camp, tampoc quedà constància de l'existència del citat registre, almenys a nivell general de l'organització.

## Àrees de Millora

| | | |
|---|---|---|
| ● | Àrea de Millora | És necessari portar-ne un registre d'entrades i sortides de suport que emmagatzemin dades de caràcter personal a partir de nivell mitjà. En aquest sentit s'haurà de fer constar:<br><br>-Tipus de suport<br>-Data i hora<br>-Emissor / receptor<br>-Nombre de suports<br>-Tipus d'informació que conté<br>-Forma d'enviament<br>-Persona responsable de recepció / entrega |

## 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 RD 1720/ 2007.***

#### Situació actual

L'entitat té inventariats els servidors i equips, si bé aquesta relació no queda dins del document de seguretat ni annex al mateix.

Pel que fa als dispositius portàtils, l'Entitat comenta que normalment són els comandaments i directius els que accedeixen a aquest tipus de suport però no s'emmagatzemen dades personals als seus disc durs. Únicament el Gerent, el responsable de SSII i el personal de l'empresa externa d'informàtica poden tenir accés a informació amb dades personals via terminal server.

Pel que fa a la destrucció de suports, l'empresa externa Ecològic s'encarrega de la destrucció dels ordinadors als quals prèviament se'ls han extret els discs durs, assegurant-se prèviament que no hi ha dades de caràcter personal. D'aquesta destrucció l'empresa certifica la seva destrucció.

Per altra banda, en tant a la destrucció de papers, existeix màquina trituradora ubicada en el segon pis de la Fundació, en el departament de Pacients; també hi ha contenidors tancats de l'empresa Ecològic repartits en vàries zones, els quals són recollits i canviats per nous quan estan plens. També, dins de l'Annex 3 s'inclou el deure de tota persona de *"destruir aquells documents que així ho requereixin perquè ja no tinguin cap utilitat i continguin dades de caràcter personal"*. S'aporta certificat de l'empresa Ecològic de la retirada i destrucció de documentació.

#### Àrees de millora

| | | |
|---|---|---|
| ? | No detectada | *Caldria que es fes la corresponent descripció d'aquests punts en el document de seguretat.* |

### 5.18. Control d'accés.

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

**Situació actual**

L'Entitat ha de vetllar perquè la informació de caràcter personal, independentment del nivell de seguretat aplicable, sigui emmagatzemada de forma segura i fora de l'abast de tercers no autoritzats. En aquest sentit, durant els treballs de camp es va observar que els despatxos, zones de treball i diferents estàncies amb dades de caràcter personals estaven dotats de sistemes de tancament els quals, al final de la jornada, quedaven tancats amb clau.

Per altra banda, a més, dins dels despatxos els armaris que podien emmagatzemar dades també estaven sota sistemes de tancament i únicament aquella informació que s'estava tramitant en aquell moment o estava pendent de revisió era la que estava sobre les taules.

L'accés al CPD de l'entitat únicament hi té accés el responsable d'IT, així com manteniment i neteja.

**Salvetat**

| | | |
|---|---|---|
| ? | No detectada | |

### 5.19. Registre d'accessos.

***Base legal: Article 113 RD 1720/2007.***

**Situació actual**

Aquesta mesura no afectaria, doncs només aplica a fitxers de nivell alt en suport documental, la qual cosa a dia d'avui no existeix en cap dels fitxers que té notificats l'Entitat.

**Salvetat**

| | | |
|---|---|---|
| ? | No detectada | |

### 5.20. Criteris d'arxiu.

***Base legal: Articles 106 RD 1720/2007.***

## Situació actual

Val a dir que a dia d'avui el suport documental que utilitza l'Entitat s'ha reduït enormement d'ençà que es fa ús del Gestor documental. Per tant, el paper del qual es disposa és temporal i queda custodiat per cada departament, en els armaris de la seva zona tancats en clau.

No es descriu la situació dels arxius en el document de seguretat. En aquest, també caldria citar de l'externalització feta a l'empresa *Casa Rojals SL*.

## Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de millora | *Cal que es descrigui la situació en què es custodia la documentació en les dependències de l'Entitat, així com també esmentar les condicions de documentació de la que s'hagi externalitzat la custòdia.* |

### 5.21. Entrades i sortides de documents.

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

## Situació actual

No es fa menció ni en el document de seguretat ni en cap altre annex al DS al registre d'entrades i sortides.

Durant els treballs de camp, tampoc quedà constància de l'existència del citat registre, almenys a nivell general de l'organització.

## Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | És necessari que l'Entitat revisi els fluxos d'informació, enviaments i recepcions d'informació a cada centre per tal d'identificar-ne els circuits i establir-ne un registre en el qual es facin constar totes les entrades i sortides de documents a partir del nivell mig. En aquest sentit s'haurà de fer constar:<br><br>-Tipus de suport<br>-Data i hora<br>-Emissor / receptor<br>-Nombre de suports<br>-Tipus d'informació que conté<br>-Forma d'enviament<br>-Persona responsable de recepció / entrega |

### 5.22. Fitxers temporals.

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

## Situació actual

Tal i com ja s'esmentava en l'anterior punt 5.17, dins de l'Annex 3 s'inclou el deure de tota persona de *"destruir aquells documents que així ho requereixin perquè ja no tinguin cap utilitat i continguin dades de caràcter personal"*.

Segons es comprovà durant els treballs de camp, tothom està conscienciat en l'ús d'aquests mecanismes per a la destrucció del paper amb dades de caràcter personal.

## 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

Com ja s'esmentava anteriorment, en el document de seguretat hi consta la definició el registre d'incidències, segons el qual, qualsevol incidència ha de comunicar-se en un termini de 24 hores al representant de la Fundació/gerent, qui es responsabilitza d'analitzar-la i valorar-ne els efectes en termini de 48 hores. Així mateix, es fa la previsió que en cas d'haver-se de comunicar a l'Agencia de Protecció de Dades, hauria de ser en termini màxim de 7 dies des de la data en què es produís la incidència.

Així mateix, es fa notar que dins del punt de funcions i obligacions del personal del mateix document de seguretat també es remarca el deure de tota persona a comunicar a la direcció qualsevol incidència o anomalia que afecti a la seguretat dels fitxers amb dades personals, la qual cosa es repeteix en el contingut de l'Annex 3 que subscriu tot treballador.

El dit registre d'incidències consta en l'Annex 2 del document de seguretat.

Malgrat l'anterior, durant el treball de camp es constatà que no existia coneixement per part del personal de com procedir davant d'eventuals incidències. Tampoc es donà evidència d'haver complimentat el citat registre d'incidències.

#### Salvetat

| | | |
|---|---|---|
| ▼ | Salvetat | Es necessari que s'implanti un procediment efectiu i real per a la gestió de les incidències que puguin ocasionar-se i que aquest procediment sigui conegut per part de tota l'organització. |

### 5.24. Difusió de funcions i obligacions.

***Base legal: Article 89.2 RD 1720/2007.***

## Situació actual

L'Entitat entrega als l'Annex 3 del document de seguretat, on s'hi descriuen els principals deures que tots tenen respecte al tractament de dades personals. No obstant, en aquest no hi ha una menció concreta a quines serien les conseqüències en cas d'incompliment.

No hi ha evidència que s'hagi fet formació en matèria de protecció de dades en els darrers 2 anys.

## Àrees de millora

| | | |
|---|---|---|
| ● | Àrea de Millora | Tenint en compte l'article 89.2 del RLOPD, cal que l'Entitat inclogui dins de l'Annex 3 les conseqüències de l'incompliment de les seves estipulacions.<br><br>Convé que l'Entitat dugui a terme formació periòdica a tot el col·lectiu que tingui accés i/o tracti dades personals. |

## 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 |
|---|
| 5.3. Document de seguretat |
| 5.4. Delegació d'autoritzacions |
| 5.9. Connexions remotes |
| 5.14. Còpies de seguretat |
| 5.16. Registre d'entrades i sortides |
| 5.20. Criteris d'arxiu |
| 5.24. Difusió de funcions i obligacions |

| SALVETATS |
|---|
| 5.5. Tercers |
| 5.6. Legitimació de dades |
| 5.7. Drets ARCO |
| 5.10. Transmissions per xarxes de telecomunicacions |
| 5.11. Control d'accés |
| 5.12. Identificació i autenticació d'usuaris |
| 5.13. Registre d'accessos |
| 5.23. Registre d'incidències |

Barcelona, 29 de desembre de 2017.

Pere Ruiz Espinós

- Soci-