# Protecció de dades de caràcter personal

Novembre de 2019
Protocol: C-12.100

## Fundació Internacional Josep Carreras

Informe d'Auditoria de protecció de dades de caràcter personal

# INDEX

## 1. OBJETIUS I CONTINGUT

El mes d'abril de 2016 es va aprovar el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades, publicat al DOUE 4.5.2016, referit en endavant com a RGPD o Reglament). Aquesta nova regulació, vehiculada per primer cop a través d'un reglament europeu, comporta canvis significatius en la protecció de dades de caràcter personal, tant des del punt de vista dels drets de les persones com de les obligacions de les persones i entitats que tracten dades de caràcter personal.

El Reglament introdueix els conceptes de privacitat des del disseny i privacitat per defecte. Això implica que el responsable ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, les mesures tècniques i organitzatives adequades concebudes per aplicar de manera efectiva els principis de protecció de dades (com, per exemple, la seudonimització), i integrar les garanties necessàries en el tractament per complir els requeriments del Reglament.

Si abans el Reglament de Desenvolupament de la LOPD (RLOPD) determinava amb detall i de forma exhaustiva les mesures de seguretat que havien d'aplicar-se segons el tipus de dades objecte de tractament, amb el RGPD els responsables i encarregats establiran les mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat en funció dels riscos detectats durant l'anàlisi prèvia.

D'altra banda, cal considerar l'aprovació relativament recent de la nova llei orgànica de protecció de dades, la Llei 3/2018, de 5 de desembre, de Protecció de Dades Personals i garanties dels drets digitals (LOPDGDD), que adapta a l'ordenament jurídic espanyol el RGPD; la nova LOPD conté una disposició derogatòria única per la qual es deroga la LOPD i qualssevol altres disposicions d'igual o inferior rang que contradiguin, s'oposin, o resultin incompatibles amb el que disposa el RGPD.

Per tot plegat, a partir de 24 de maig de 2018:

- Resulta plenament aplicable allò previst al RGPD, i a la Llei Orgànica 3/2018, LOPDiGDD (a partir del 7 de desembre de 2018).
- Correspon al responsable o encarregat del tractament aplicar les mesures tècniques i organitzatives adequades per garantir que només es tracten les dades personals necessàries per a cada finalitat específica del tractament. Per a determinar les mesures tècniques i organitzatives s'atendrà a:
    - El cost de la tècnica
    - Els costos d'aplicació
    - La naturalesa, l'abast, el context i les finalitats del tractament
    - Els riscos pels drets i llibertats
- La falta de determinació per part del responsable o encarregat del tractament de les mesures de seguretat suposa l'incompliment del principi de responsabilitat proactiva.

- A falta de concreció per part del responsable o encarregat del tractament de mesures específiques, s'auditarà atenent a l'esquema de mesures de seguretat previst al RLOPD, sempre que sigui compatible i no contrari al RGPD ni a la LOPDiGDD. Les mesures previstes al RLOPD que ja estiguin implantades poden ser útils, però cal analitzar en cada cas si són suficients o és necessari modificar-les.
- 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. Es tindran en compte les consideracions de l'AEPD en relació a les mesures indispensables que s'ha de complir amb els tractaments d'escàs risc.

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.

## 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, S.L. 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** | Fundació Internacional Josep Carreras (FIJC) |
| **CIF** | G-58734070 |
| **Domicili** | C/ Muntaner, 383, 2n<br><br>08021 Barcelona |

### 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, la investigació de noves tècniques per a combatre aquesta malaltia, l'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 a la web corporativa http://www.fcarreras.org/ca

## 3.2. TREBALLS EFECTUATS

S'han realitzat els treballs de camp de l'auditoria en diferents àrees i serveis de l'entitat:

- Delegació de Protecció de Dades
- Informàtica
- Pisos
- Pacients
- Coordinació Tècnica
- Direcció Mèdica
- Coordinació REDMO
- Qualitat i Compliance
- Actes Benèfics
- Secretaria i Atenció al Públic
- Administració del REDMO
- Cordons i Workups

- Donants
- Fidelització
- Administració de socis
- Comunicació i màrqueting
- Revisió d'ubicacions físiques: oficines, tancaments, sala de servidors, etc.

També, s'han revisat personalment les ubicacions físiques de l'entitat, especialment oficines, tancaments i sala de servidors.

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

| | |
|---|---|
| **Dies** | 14 i 15 de novembre de 2019 |

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

Persones entrevistades per ordre d'intervenció:

| NÚMERO | PERSONA ENTREVISTADA | CÀRREC O ÀREA DE TREBALL |
|---|---|---|
| 1 | Sra. Iris Bargalló | Delegada de protecció de dades (DPD) |
| 2 | Sra. Anna Giner | Qualitat i Compliance |
| 3 | Sr. Mario Gran | Sistemes d'informació |
| 4 | Sra. Esther Soto | Pisos d'acollida |
| 5 | Sra. Mavi Díaz | Pacients |
| 6 | Sra. Cristina Fusté | Coordinació Tècnica REDMO |
| 7 | Sra. Núria Marieges | Coordinació REDMO |
| 8 | Dra. Juliana Villa | Direcció mèdica |
| 9 | Sra. Clàudia Nogués | Gestió d'actes benèfics |
| 10 | Sra. Regina Díez | Gestió d'actes benèfics |
| 11 | Sra. Tina Grau | Coordinadora de Socis, Donatius i Herències |
| 12 | Sra. Adriana Bararu | Secretaria General |
| 13 | Sra. Raissa Dardet | Administració REDMO |
| 14 | Sra. Carolina Salillas | Administració REDMO |
| 15 | Sr. Jordi Martínez | Àrea de workups |
| 16 | Sra. Isabel Monteagudo | Àrea de worrkups |
| 17 | Sra. Cecilia Montesinos | Àrea de workups |
| 18 | Sra. Montserrat Rebagliato | Àrea de cordons per a pacient internacional |

| | | |
|---|---|---|
| 19 | Sra. Núria Giménez | Àrea de donants |
| 20 | Sra. Cristina Bueno | Àrea de donants |
| 21 | Sra. Mireia Bel | Àrea de fidelització |
| 22 | Sra. Anna Grau | Administració de socis |
| 23 | Sra. Marta Fernández | Comunicació i màrqueting |
| 24 | Sra. Inés Martí | Comunicació i màrqueting |
| 25 | Sra. Alexandra Carpentier de Changy | Comunicació i màrqueting |

Relació de la documentació lliurada a l'auditor:

- Estatuts de la Fundació Internacional Josep Carreras.
- Organigrama nominal de juliol de 2019.
- Acta de reunió de Patronat de 25/04/2019 en què es ratifica el nomenament de la DPD, que va tenir lloc el juny de 2018.
- Justificant de la comunicació del nomenament de la DPD a l'AEPD.
- Comunicació de l'AEPD confirmant la inscripció del DPD.
- Certificats de formació de la DPD en matèria de protecció de dades.
- Informe de progrés RGPD FIJC.
- Registre d'activitats de tractament.
- Contractes d'encàrrec de tractament de dades: Wesser & Partner, S.L. i PLC-EPI, S.L.
- Acord de transferència i ús de dades entre membres de la World Marrow Donor Association (WMDO).
- Acord de transferència i ús de dades entre la World Marrow Donor Association (WMDO) i la Spanish Bone Marrow Donor Registry (REDMO).
- DF-036 Procediment Drets dels Interessats.
- DF-037 rev.01 Guia drets dels Interessats.
- IMP-060 v.01 Drets Afectats (circuit i formularis).
- DF-035 rev.01 Procediment Violacions de seguretat de Dades Personals.
- Formulario notificación brechas de seguridad AEPD.
- IMP-057 v1 Formulari notificació incidència seguretat interessat.
- DF-019 rev 01 - Matriu Avaluació Riscos.
- DF-032 rev.01 Politica de Privacitat del Personal FJC.
- DF-033_Codi_Conducta_Seguretat_Informaciov1.
- Consentiments de REDMO: Informació sobre donació de medul·la òssia de progenitors hematopoètics, Informació sobre donació de sang perifèrica, Consentiment informat per a donants de progenitors hematopoiètics (4 idiomes).

- Document de seguretat TIC v.1.0.
- Registre Usuaris (Excel).
- Pla de recuperació de desastres.
- Symantec - Data Sheet: Endpoint Security.
- DocuWare Cloud  (White Paper).
- DocuWare RGPD  (White Paper).
- DocuWare Security  (White Paper).
- Conveni pisos d'acollida.
- Informació i compromís dels treballadors.
- Informe Avaluació d'Impacte - WhatsApp (en procés de revisió)

## 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 no conformitat 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. |
| ▼ | **No conformitat**, 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: Article 24.1 RGPD

**Situació actual**

D'acord amb l'article 24.1 del RGPD, correspon al responsable del tractament aplicar les mesures tècniques i organitzatives necessàries a fi de garantir i poder demostrar que el tractament és conforme al mateix RGPD. A més, aquestes mesures es revisaran i s'actualitzaran sempre que sigui necessari. Per aquest motiu, FIJC encarrega la realització d'aquest informe d'auditoria, que serà analitzat pel responsable del tractament i elevat a direcció, per tal que s'adoptin les mesures correctores adients.

L'entitat ja té implementada una política de realització biennal d'auditories sobre protecció de dades. La darrera auditoria sobre protecció de dades que es va realitzar és de data 29 de desembre de 2017.

S'aporten diferents evidències del compliment d'aquesta mesura de seguretat. El Document de Seguretat TIC consta com a actualitzat, signat i validat pel Gerent de l'entitat a data 25/10/2019, i assumeix explícitament el compromís de realitzar una auditoria biennal com a mesura de seguretat. Un altre document aportat, el titulat "*Informe de Progrés RGPD*", de 05/04/2019, incorpora també un pla d'auditories destinades al compliment normatiu. D'altra banda, l'acta de reunió del Patronat de 25/04/2019 conté un informe de compliment de la legislació sobre protecció de dades.

**No detectada**

| | |
|---|---|
| ▲ | |

## 5.2. REGISTRE D'ACTIVITATS DEL TRACTAMENT

Base legal: Article 30 RGPD

**Situació actual**

L'article 30 del Reglament General de Protecció de Dades (RGPD) estableix l'obligatorietat de realitzar el Registre d'Activitats del Tractament (RAT). Aquesta obligació no afectarà aquelles organitzacions que tinguin menys de 250 treballadors, llevat que el tractament de les dades que facin pugui comportar un risc per als drets i les llibertats dels interessats, no sigui ocasional, o inclogui categories especials de dades o dades personals relatives a condemnes i infraccions penals.

Les dades que tracta l'entitat inclouen dades de categoria especial, com ho són per exemple les dades de salut dels pacients i dels donants. En aquest sentit i, en aplicació de les previsions del RGPD, l'entitat està obligada a elaborar i mantenir un Registre d'Activitats de Tractament.

A data de l'auditoria, FIJC manifesta que ja ha elaborat un RAT, que aporta per a la seva revisió i que, tal com es pot comprovar, identifica tractaments de dades diferents amb els noms següents:

- Donantes médula
- Workups
- Pacientes
- Cordones
- Gestió Econòmica REDMO
- Socios
- Amics
- Personal
- Posibles
- Clientes y proveedores
- Blanqueo de capitales
- Tienda on-line
- Iniciatives solidàries
- Pisos d'Acollida
- Testimonis
- Participants d'Activitats de la FIJC
- Aliances Corporatives

El RAT ha estat elaborat com a document Excel. Es comprova que efectivament ja conté tots els camps previstos per l'article 30 RGPD i que, de fet, conté camps addicionals, com ara la identificació dels departaments que accedeixen a cada tractament o els drets que poden exercir els interessats en cada cas.

Fins a l'entrada en aplicació del RGPD, l'entitat tenia ja diferents fitxers notificats, que es correspondrien en part amb els actuals tractaments de dades identificats al RAT amb el mateix nom. En tot cas, és important assenyalar que l'activitat principal desenvolupada per FIJC, la que implica un tractament més massiu i sensible de dades, és la corresponent a la gestió de les donacions i transplantaments de materials biològics.

D'acord amb la disposició final onzena de la LOPDGDD, que modifica l'article 6 bis de la Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern, els

subjectes del sector públic citats a l'article 77.1 de la LOPDGDD tenen l'obligació addicional de publicar el seu RAT i fer-lo accessible electrònicament. L'entitat, però, no es troba entre els subjectes obligats de l'article 77.1 de la LOPDGDD.

## Àrees de millora

| | |
|---|---|
| 🟡 | El RAT elaborat per FIJC reflecteix i identifica de forma correcta els tractaments realitzats per l'entitat i, en aquest sentit, és bàsicament conforme a les previsions de l'art. 30 RGPD. És particularment encertada la identificació de les bases jurídiques, que demostra haver-se fet després d'una reflexió significativa, i cal assenyalar especialment l'aparició de l'interès vital com a base jurídica alternativa en determinats tractaments, que, d'acord amb els procediments de donació i transplantament, revesteixen efectivament un caràcter d'urgència.<br><br>Com a àrea de millora assenyalem alguns aspectes que poden contribuir a una millor expressió del RAT, que són els següents:<br><br>• Categoria d'interessats: En aquesta camp del RAT hem d'identificar els col·lectius de persones de qui tenim dades, no la font de les dades. Observem que en alguns pocs tractaments hi ha aquesta confusió. Així, per exemple, en els tractaments de "Cordons", "Gestió econòmica Redmo" i "Aliances corporatives" s'hi identifiquen ara en aquest camp el "Banc de Cordons", "Registres i Hospitals" i "Internet i compra de base de dades" respectivament, quan haurien de referir-s'hi els col·lectius de "donants de cordons", "pacients" i "donants" i "representants d'altres organitzacions" respectivament.<br><br>• Drets dels interessats: En aquest camp del RAT s'ha optat per a indicar que, en relació a determinats tractaments de dades, no operen determinats drets (així, per exemple, en els tractaments de "Cordons" i "Gestió econòmica Redmo", només s'hi identifiquen els drets d'accés i rectificació). És correcte adaptar el RAT i incloure-hi la informació que es consideri necessària per tal d'optimitzar-lo com a document intern de treball. Tot i que evidentment hi ha una reflexió darrere aquesta decisió vinculada a la realitat del tractament, recomanem no perdre de vista que, d'entrada, tots els drets operen en tots els tractaments de dades, d'acord amb la seva configuració per part del RGPD.<br><br>• Destinataris de les dades: Caldria incorporar un camp de destinataris de les dades, d'acord amb l'art. 30.1.d) RGPD. Ara com ara hi ha un camp al RAT sobre seguretat en les transferències internacionals de dades, que proporciona una informació correcta, però no hi ha un camp que identifiqui totes aquelles organitzacions o categories d'organitzacions a què es transfereixin dades de forma habitual, bé sigui a nivell nacional, bé sigui a nivell internacional.<br><br>Tot i que el criteri actualment aplicat a l'hora de definir els diferents tractaments és correcte i ajustat al RGPD, recomanem simplificar i reagrupar alguns dels tractaments, tenint en compte la finalitat de cadascun d'ells i el tipus de dades tractades. Alguns tractaments actualment identificats podrien ser en realitat |

| | |
|---|---|
| | aspectes d'un mateix tractament, i seria possible identificar-los com a tal. En particular, plantegem que es valori la possibilitat d'agrupar alguns dels tractaments segons l'esquema següent:<br><br>• Donants / Gestió de donacions – Dins aquesta activitat de tractament hi podríem incloure els tractaments actualment identificats com a "donants de medul·la", "workups" i "cordons", ja que tots ells responen a la finalitat de gestionar un procediment de donació, encara que després aquest procediment difereixi en funció del tipus de donació.<br><br>• Clients i proveïdors: El tractament de dades "Botiga on-line" es podria incloure dins aquest tractament de "Clients i proveïdors", ja que la botiga no deixa de ser un dels diferents canals de venda més que no pas un tractament diferenciat. |

### 5.3. DEFINICIÓ DE LES MESURES PER PART DEL RESPONSABLE DEL TRACTAMENT

Base legal: Articles 24, 25 i 32 RGPD

**Situació actual**

El RGPD, a diferència del RLOPD, no preveu mesures específiques per a la seguretat del tractament de les dades personals, sinó que deixa en mans del responsable del tractament la definició i implementació de les mesures més adequades d'acord amb els riscos que plantegi cada tractament de dades. L'article 25 RGPD contempla les obligacions de la protecció de dades des del disseny i per defecte. Sobre les mesures que cal aplicar, s'estableix:

- Es manté un deure d'aplicar les mesures tècniques i organitzatives adients amb la finalitat de garantir que el tractament sigui conforme al RGPD.
- Les mesures adoptades pel responsable del tractament han de ser demostrables.
- Caldrà revisar periòdicament i actualitzar aquestes mesures, quan sigui necessari.
- Cal tenir present sempre el principi de protecció de dades des del disseny i per defecte.

No consta cap evidència que l'entitat hagi adoptat formalment mesures de seguretat que siguin una alternativa a les mesures de seguretat del RLOPD i que siguin diferents a les aplicades fins al 24 de maig de 2018.

El RGPD no impedeix que les mesures de seguretat previstes pel RLOPD continuïn aplicant-se, per tal de garantir el compliment de les obligacions del responsable del tractament. En aquest sentit, l'entitat continua aplicant les mesures de seguretat identificades als Documents de Seguretat i en d'altres documents, a més de voler complir els nous requeriments del RGPD, com ara el nomenament del DPD o l'elaboració d'un RAT, entre d'altres.

L'AEPD defineix unes mesures mínimes obligatòries per a aquells tractaments de dades que suposin un risc escàs. Aquestes mesures, de tipus organitzatiu i tècnic, cal garantir-les en tot cas i sobre tots els tractaments. L'entitat assumeix aquestes mesures al Document de Seguretat TIC i els seus annexos i en d'altra documentació aportada durant aquesta auditoria, com, per exemple, l'Informe de progrés RGPD FIJC. Es valora especialment que el Document de Seguretat ha estat aprovat i signat pel Gerent de l'entitat.

| **MESURES ORGANITZATIVES** | |
|---|---|
| Deure de confidencialitat i secret | Evitar l'accés de persones no autoritzades a les dades personals: evitar pantalles desateses, documents en zones d'accés públic, etc. Quan s'absenti del lloc de treball es procedirà al bloqueig de l'estació o tancament de la sessió. |
| | Els documents en paper i suports electrònics s'emmagatzemaran en lloc segur (armaris, calaixos o estances d'accés restringit). |
| | No es llençaran documents o suports electrònics amb dades personals sense garantir-ne la destrucció. |

| | |
|---|---|
| | No es comunicaran dades personals o qualsevol informació personal a tercers. |
| | Signar amb els treballadors que tinguin accés a dades un acord de confidencialitat i entregar-los un manual per a usuaris amb les obligacions i mesures establertes. |
| | El deure de secret i confidencialitat es manté fins i tot després de finalitzar la relació laboral del treballador amb l'empresa. |
| Drets dels titulars de les dades | S'informarà als treballadors, sobretot als que puguin estar de cara al públic, sobre el procediment d'atenció als drets dels interessats, definint de forma clara els mecanismes previstos per a l'exercici d'aquests drets. |
| | Prèvia presentació del DNI o passaport, les persones interessades podran exercir els seus drets. El responsable del tractament haurà de donar d'atendre les seves peticions. |
| Violacions de seguretat de les dades | Quan es produeixin violacions de seguretat, es notificaran a l'autoritat de control en el termini de 72 hores d'ençà del moment que se'n té coneixement. La notificació es realitzarà a través de la seu electrònica de l'autoritat de control. |
| | Es podrà gestionar de forma interna un registre d'incidències que es puguin produir amb dades personals. |
| Documentació paper | S'establiran criteris d'arxiu per a la documentació que contingui dades de caràcter personal, i es custodiarà de forma adequada, quan no es faci servir. |
| | Categories especials de dades: es restringirà l'accés a aquest tipus de documentació, s'habilitaran mètodes per a la seva destrucció i es durà a terme un registre d'accés a aquests documents. |
| Delegat de Protecció de Dades | ✓ El tractament el realitzi una autoritat o organisme públic<br>✓ Les activitats consisteixin en operacions que, degut a la seva naturalesa, abast i/o fins, requereixin una observació habitual i sistemàtica d'interessats a gran escala.<br>✓ Les activitats principals consisteixin en el tractament a gran escala de categories especials de dades personals i de dades relatives a condemnes i infraccions penals. |

| MESURES TÈCNIQUES | |
|---|---|
| Identificació | S'establiran mecanismes d'autenticació personalitzats per accedir als sistemes mitjançant, per exemple, un usuari i contrasenya específics per a cada treballador (identificació inequívoca). |
| | S'establiran perfils d'usuaris amb diferents nivells d'accés a dades personals segons les funcions del treballador. |
| | Quan un dispositiu s'utilitzi per al tractament de dades personals i fins d'ús personal, es recomana establir perfils diferents. |
| | Es recomana disposar de perfils amb drets d'administració per a la instal·lació i configuració del sistema i usuaris sense privilegis. |
| | Es garantirà, com a mínim, l'existència de contrasenyes per a l'accés a les dades personals emmagatzemades als sistemes. La contrasenya tindrà almenys 8 caràcters (números i lletres) i l'empresa decidirà la complexitat d'aquestes claus. Es canviaran les claus, com a mínim, un cop l'any. |
| | Cal garantir la confidencialitat de les contrasenyes, evitant que puguin ser exposades a tercers. |
| | En cas de intents d'accés fallits a un compte d'usuari es bloquejarà aquest compte. |
| Deure de salvaguarda | Els dispositius i ordinadors utilitzats per a l'emmagatzemament i el tractament de les dades personals hauran de mantenir-se actualitzats. |
| | En aquests dispositius es disposarà d'un sistema d'antivirus instal·lat i degudament actualitzat. |
| | Per evitar accessos remots indeguts a les dades personals es prendran les mesures corresponents com l'existència de Firewall. |
| | Periòdicament (mínim setmanal) es duran a terme processos de còpia de seguretat de les dades personals en un suport diferent al que s'utilitza per al treball diari. Es disposarà d'una còpia de seguretat en un lloc diferent d'on s'emmagatzemen les dades. |
| | Categories especials de dades: es durà a terme un registre d'accessos d'aquest tipus de dades. |

| | |
|---|---|
| Gestió de suports i dispositius | Es disposarà d'un inventari actualitzat dels diferents suports/dispositius que continguin dades personals. |
| | Categories especials de dades: quan calgui realitzar l'extracció de dades personals fora del recinte on se'n fa el tractament, ja sigui per mitjans físics o electrònics, s'haurà de valorar la possibilitat d'utilitzar un mètode d'encriptació. |
| | S'establiran mecanismes de restricció d'accés a la sala on es trobin els servidors (CPD). |
| | Com a norma general, els fitxers que continguin dades personal s'emmagatzemaran en un servidor de fitxers i no en els dispositius dels usuaris de forma local. |

El compliment d'aquestes mesures mínimes serà analitzat detalladament en apartats posteriors del present informe.

Els tractaments que realitza FIJC a data de l'auditoria són, en termes generals, els mateixos que realitzava anteriorment a l'entrada en aplicació del RGPD el 25 maig de 2018, de manera que les mesures de seguretat ja van ser definides i implementades sota l'anterior règim legal, tenint en compte les característiques i els riscos d'aquests mateixos tractaments. En particular, s'havien tingut en compte els tractaments de dades de donants i pacients, sobretot de dades de salut, però també de genètica i de circumstàncies personals, entre d'altres, que deriven dels serveis prestats per l'entitat. Aquests tractaments suposen tractar dades de categoria especial i impliquen un risc rellevant.

Tal com s'ha pogut comprovar amb la documentació aportada, ja s'ha realitzat un informe d'anàlisi de riscos i d'avaluació d'impacte sobre l'ús de l'aplicació de missatgeria instantània WhatsApp, com a expressió de la responsabilitat proactiva que té l'entitat en la gestió del risc.

## Àrees de millora

| | |
|---|---|
| ● | No hi ha constància documental d'haver-se adoptat mesures de seguretat diferents o alternatives a les previstes en l'antic règim legal del RLOPD de 2007; sí que s'aporten, tanmateix, un document de seguretat, annexos i protocols que demostren i evidencien l'adopció i aplicació per part de l'entitat de mesures de seguretat adequades, aprovats en bona part per la gerència de l'entitat. És important que aquesta documentació estigui sempre actualitzada i que estigui sempre validada formalment pel responsable del tractament.<br><br>Cal fer sempre una revisió de les mesures de seguretat i circuits existents per tal de corroborar que són adequats als requeriments legals del RGPD; en particular, cal prioritzar els principis de privacitat per disseny i per defecte en les mesures de seguretat i circuits de tractament que s'estiguin aplicant. També cal considerar la realització d'anàlisis de riscos i avaluacions d'impacte en relació a tractaments de dades que impliquin un alt nivell de risc per als drets i llibertats de les persones, també especialment quan es pretengui aplicar noves tecnologies en el seu |

| | |
|---|---|
| | tractament. Hem d'entendre tot això també vinculat a l'obligació que té l'entitat de gestionar el risc en general i el principi de responsabilitat proactiva.<br><br>D'acord amb la documentació aportada, ja s'ha realitzat correctament una anàlisi de riscos i avaluacions d'impacte per a un determinat tractament vinculat a la implantació d'una nova tecnologia, com és el cas, per exemple, de l'ús del WhatsApp.<br><br>En el cas dels tractaments de dades derivats dels serveis prestats per l'entitat i que impliquen disposar de dades de salut de donants i pacients, no cal dir que presenten un nivell de risc rellevant i impliquen el tractament de dades de categoria especial; en quests casos, és molt convenient realitzar avaluacions d'impacte sempre que sigui necessari, ja que compleixen els criteris de la llista de tractaments especificats per l'AEPD.<br><br>Les autoritats de control han publicat guies sobre criteris i metodologia a emprar en l'anàlisi de riscos i l'elaboració d'avaluacions d'impacte, tant l'Agència Espanyola de Protecció de Dades (AEPD) com l'Autoritat Catalana de Protecció de Dades (APDCAT). També recentment l'AEPD ha publicat una eina online sobre la matèria que s'anomena GESTIONA. Degut a la complexitat d'aquests informes, el més habitual és encarregar-ne l'elaboració a empreses o entitats especialitzades, sota la supervisió del DPD de l'entitat. D'altra banda, cal tenir en compte que no seria correcte que sigui la DPD qui elabori directament els informes d'avaluació d'impacte, ja que això planteja problemes de compatibilitat amb les seves funcions d'assessorament i supervisió. |

### 5.4. DELEGAT DE PROTECCIÓ DE DADES

Base legal: Article 37 RGPD

**Situació actual**

Segons la informació i evidències proporcionades, l'entitat va procedir a nomenar la Sra. Iris Bargalló Arraut com a delegada de protecció de dades (DPD) el mes de juny de 2018. El nomenament va ser ratificat per la Junta de l'entitat el passat abril de 2019, tal com es pot comprovar amb l'acta aportada. D'altra banda, es va comunicar aquest nomenament tant a l'Agència Espanyola de Protecció de Dades (AEPD). S'aporten com a evidències l'acta de nomenament signada per Gerència, la notificació enviada a l'AEPD en data 29/06/2018 i la resposta de confirmació enviada per l'AEPD, que porta la data 06/10/2019.

Com a acció de difusió del nomenament de la DPD, es va realitzar una presentació pública de la DPD i de les seves funcions davant de tot el personal (aproximadament, unes 30 persones).

L'existència de la DPD ja consta a l'organigrama de l'entitat, tal com es pot confirmar amb el document d'organigrama aportat.

La DPD és una professional externa de FIJC que hi presta exclusivament tasques corresponents al càrrec. Té coneixements jurídics acreditats i demostrada formació i experiència en matèria de protecció de dades. En aquest sentit, s'han aportat certificats d'AENOR i de l'Agència Espanyola del Medicament relatius a la realització de cursos especialitzats sobre protecció de dades en relació al RGPD i a la LOPDGDD. Com que no té altres funcions que impliquin la presa de decisions sobre el tractament de les dades que realitza l'entitat, el càrrec de DPD resulta compatible i sense conflicte d'interès.

La DPD ja s'ha constituït en responsable de la coordinació de la formació sobre protecció de dades a l'entitat i, com a exemple, ha elaborat un document audiovisual sobre el nou RGPD i un qüestionari que s'ha difós entre tot el personal. També ha organitzat dues sessions presencials de formació.

La DPD ha elaborat un pla de treball, que proposa diferents mesures a implementar en els propers mesos. Bona part d'aquest pla està detallat al document "*Informe de progrés RGPD FIJC*", de data 05/04/2019.

Confirmem que, en general, els textos legals que fa servir l'entitat per a informar sobre el tractament de les dades, de conformitat amb l'art. 13 RGPD, ja informen també sobre l'existència de la DPD i la possibilitat de comunicar-s'hi.

**No detectada**

| | |
|---|---|
| ▲ | |

## 5.5. ENCARREGATS DE TRACTAMENT I PROVEÏDORS SENSE ACCÉS A DADES.

### ENCARREGATS DE TRACTAMENT

Base legal: Article 28 RGPD i disposició transitòria cinquena LOPDGDD

**Situació actual**

El mateix document Excel "*Registre d'Activitats del Tractament*", aportat a aquesta auditoria ja conté en una de les seves pestanyes una relació actualitzada d'encarregats de tractament, de manera que l'entitat pot saber en qualsevol moment quines relacions hi ha d'accés a dades per part d'encarregats i el tipus de contracte que hi té signat, si està actualitzat o està pendent d'actualització.

D'altra banda, un cop revisada una mostra de contractes d'encàrrec de tractament de dades personals, fem els següents comentaris al respecte:

| ET DETECTATS | SERVEI PRESTAT | CON-TRAC-TE | COMENTARIS |
|---|---|---|---|
| **Wesser & Partner, S.L.** | Captació de socis cara a cara, realització de campanyes i gestió telefònica de socis | ✓ | El contracte d'encàrrec de tractament de dades, signat el 31/03/2016, no contempla totes les previsions del RGPD (art. 28), la relació és correcta, en aplicació de la moratòria legal. |
| **PLC-EPI, S.L.** | Serveis informàtics | ✓ | El contracte signat és conforme al RGPD. |
| **NTI Figueras, S.L.** | Gestió de comunicació amb els socis i enviament de certificats de la renda als col·laboradors. | ✓ | El contracte d'encàrrec de tractament de dades, signat el 31/03/2016, aplica l'antiga LOPD. Per tant, tot i no contemplar les previsions del RGPD (art. 28), la relació és correcta, en aplicació de la moratòria legal. |

Segons disposa la Disposició transitòria cinquena de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals, els contractes anteriors al 25 de maig de 2018, redactats d'acord amb l'antiga LOPD i que no hagin estat actualitzats o adaptats al RGPD, es mantindran vigents fins al final i, si són per termini indefinit, fins al 25 de maig de 2022. Durant aquesta vigència, qualsevol de les parts signants podrà requerir l'altra per tal de signar un nou contracte que sigui conforme al RGPD. Tot i que és possible deixar passar els terminis, el més recomanable és procedir ja a actualitzar tots els contractes d'encàrrec de tractament de dades de conformitat amb el RGPD.

A partir del 25 de maig de 2018 tots els nous contractes amb Encarregats de Tractament han de respectar el contingut que preveu l'article 28 del RGPD.

Es revisen també que els acords de transferència i ús de dades entre membres de la World Marrow Donor Association (WMDO) i entre aquesta entitat i la Spanish Bone Marrow Donor Registry (REDMO). En aquests acords, tot i que no són ben bé d'encàrrec de tractament de dades sinó més aviat de transferència, ja es contemplen correctament les previsions del RGPD.

En qualsevol cas, cal que es revisin totes les situacions de serveis prestats per proveïdors o tercers que impliquin tractar i/o accedir a dades, ja que requereixen la signatura d'un contracte específic de tractament de dades. És important que la definició dels serveis que presten aparegui al contracte de manera precisa i transparent, de forma que s'entengui quins són els serveis que presta l'encarregat, els quals justifiquen i acoten el tractament de les dades.

**No detectada**

| | |
|---|---|
| ▲ | Es comprova que l'entitat du a terme una activitat proactiva en la gestió dels contracte d'encàrrec de tractament i que té diferenciats correctament els proveïdors que accedeixen a dades dels que no. En el cas dels que accedeixen a dades i són encarregats de tractament, ja està duent a terme un control sobre el tipus de contracte signat, procurant actualitzar els contractes anteriors al RGPD i aplicant un model de contracte d'encarregat nou, ajustat al RGPD, per als nous contractes. |

**PRESTACIONS SENSE ACCÉS A DADES**

Base legal: Article 24 RGPD

## Situació actual

Entre la documentació facilitada per l'entitat, i especialment el document Excel "*Registre d'Activitats de Tractament*", comprovem que ja es fa una relació de proveïdors de l'entitat, diferenciant que els que tenen accés a dades dels que no. Tot i que això demostra que ja s'ha fet una reflexió sobre quins proveïdors no tenen accés a dades i se'ls ha identificat en una llista, no consta que hi hagi un procediment per a fer-los signar un model de compromís de confidencialitat o clàusula de confidencialitat.

No consta entre la documentació aportada que hi hagi un model de clàusula o compromís de confidencialitat que es faci signar als proveïdors sense accés a dades.

## Àrees de millora

| | |
|---|---|
| 🟡 | D'acord amb l'art. 24 RGPD, forma part de la responsabilitat del responsable del tractament aplicar les mesures de seguretat més adequades per a assegurar-se que no hi ha accessos ni tractaments indeguts de les dades. En aquest sentit, si hi ha proveïdors que, sense tenir un accés autoritzat a les dades, per la naturalesa del servei que presten, poden tenir un accés involuntari o accidental a dades de caràcter personal (per exemple, serveis de neteja), és molt recomanable fer-los signar un compromís de mantenir la confidencialitat sobre la informació a què puguin tenir accés. |

## 5.6. LICITUD DEL TRACTAMENT, BASE JURÍDICA, INFORMACIÓ I CONSENTIMENT

Base legal: Articles 5, 6, 7, 8, 9, 10, 11, 12, 13 i 14 RGPD

**Situació actual**

S'analitza a continuació, de manera general, la legitimitat de les grans activitats de tractament de dades que du a terme l'entitat, de la qual deriven els diferents tractaments identificats al RAT. Tenim en compte, a aquest efecte, els tipus d'interessats de qui es recullen dades i les finalitats.

- **Donants de medul·la / Donants de cordons / Workups:**

  FIJC recull i tracta dades de donants de materials biològics, i d'això deriva que l'entitat hagi de recollir i tractar dades de categoria especial, especialment de salut i genètiques. La licitud i base jurídica del tractament és el consentiment de l'interessat, d'acord amb l'art. 6.1.a) del RGPD. De forma alternativa, el RAT identifica per a aquest tractament l'article 6.1.d) com a base jurídica, que és l'interès vital del pacient. Entenem que aquesta apreciació és correcta, sobretot si tenim en compte la urgència que regeix sovint el procés de transplantament, amb risc real per a la vida del pacient. En qualsevol cas, la finalitat és avaluar la compatibilitat dels donants amb pacients, a fi que es puguin realitzar finalment els transplantaments necessaris.

  Els donants es poden voler registrar als bancs de sang o centres de salut i allà inscriure's al REDMO, que és el registre que fa servir l'entitat per a la gestió de les dades dels donants i pacients. A Catalunya, en concret, els donants han d'anar al Banc de Sang i de Teixits per a inscriure's al REDMO.

  El REDMO permet fer anàlisi i classificar per edat, sexe i població, però generalment només per a finalitats estadístiques. No es fan classificacions dels donants segons perfils, ni hi ha una activitat d'elaboració de perfils.

  Són els centres corresponents als donants (bancs de sang i centres de salut on s'han registrat, aproximadament un centenar) els que tenen la responsabilitat d'actualitzar les dades al REDMO (per exemple, si un donant es mor). Per a mantenir una comunicació entre els centres i el REDMO es fa servir l'aplicació anomenada "web professional". Actualment, aquesta web ja permet la comunicació per canals segurs.

  Quan el donant inscrit és seleccionat per a convertir-se en donant efectiu i ha de sotmetre's, per tant, a proves mèdiques, és quan des del centre de salut de referència o el banc de sang li fan signar el consentiment exprés per a ser donant, que ja inclou una informació sobre protecció de dades de FIJC que és fonamentalment conforme a l'art. 13 RGPD, amb alguns aspectes millorables (en concret, caldria incidir en el fet que la FIJC és el responsable del tractament i esmentar-ho explícitament, i fer referència també als drets de limitació i portabilitat (i canviar "cancel·lació" per "supressió") en l'apartat sobre l'exercici dels drets. En qualsevol cas, observem també que els models de consentiment ja inclouen també un enllaç a la pàgina "Política de privacitat REDMO", on ja hi ha una informació exhaustiva, entenedora i completa sobre el tractament de les dades, que és conforme a l'art. 13 RGPD.

- **Pacients:**

  Les dades dels pacients es tracten generalment als centres i sistemes de salut d'acord amb una base jurídica específica del RGPD per a la prestació d'assistència sanitària, que és la corresponent a l'art. 9.2.h) RGPD. No obstant, en aquest cas, la base jurídica que FIJC identifica al seu RAT és la de l'art. 6.1.c), la protecció d'interessos vitals. Tot i que aquesta base jurídica no és incorrecta, també és cert que l'entitat participa de la prestació assistencial a través dels diferents acords que té amb les autoritats sanitàries autonòmiques i estatals i, per tant, el tractament de dades que fa es pot emparar també en l'art. 9.2.h.) RGPD. En qualsevol cas, la finalitat del tractament és la consecució d'un transplantament en relació a un pacient que el necessita urgentment.

  D'acord amb les informacions proporcionades, les peticions amb les dades de pacients venen dels centres de transplantaments que cerquen un donant no emparentat. Llavors és quan, després de comprovar que la petició reuneix tots els requisits necessaris, s'inicia el procediment de recerca. La petició arriba generalment amb les següents dades: nom del pacient, centre de transplantament, centre del sol·licitant (si són espanyols), el codi postal, la malaltia, l'estat viral (CVM) la data de naixement, el grup sanguini, l'etnicitat i les dades biomètriques. Aquestes dades són totes elles necessàries per a poder seleccionar el donant adequat a través del software EMDIS i del portal de la WMDA (associació mundial de donants de moll de l'os i sang de cordó). La transferència internacional que pot derivar d'aquesta situació està legitimada pels acords signats entre el REDMO i els altres registres, i el REDMO i la WDMA, que ja contenen previsions expresses de compliment del RGPD i de realitzar les transferències internacionals en les condicions de seguretat previstes per aquest Reglament.

  És important assenyalar que el codi postal del pacient serveix per a generar el codi amb què s'identificarà el pacient i aplicar una mesura de seudonimització a l'àrea de pacients.

  Com a reflexió a fer sobre la necessitat i proporcionalitat del tractament, cal tenir en compte l'obligació legal que donant i pacient no arribin mai a tenir coneixement un de l'altre. Això deriva també en una separació tècnica i funcional entre l'àrea dedicada a pacients i la dedicada a donants. Aquesta separació, per a major seguretat, hauria d'implicar teòricament que les persones vinculades a l'àrea de donants només haurien de tenir accés a les dades d'identitat dels donants i a les seudonimitzades dels pacients, i a la inversa. No obstant, això no és així: en la preparació de workups (planificació del trasplantament amb el donant) es té sempre coneixement del nom del pacient, malgrat que es treballi amb un codi. Això es basa, segons les informacions proporcionades, en la necessitat d'evitar riscos o errors en la identitat dels pacients, però no resulta justificat. Caldria que efectivament hi hagués aquesta separació funcional de forma efectiva, i que hi hagués un procés de seudonimització amb garanties de seguretat que suposés que a l'àrea de pacients només tenen accés a dades de donants seudonimitzades, i a l'àrea de donants només accedeixen a dades seudonimitzades dels pacients. Seria molt recomanable que l'entitat treballés en aquesta línia, per tal que el tractament de dades s'ajustés a criteris de proporcionalitat, minimització i adequació a la finalitat.

- **Pisos d'acollida**

  La finalitat del tractament és la prestació d'un servei de pisos d'acollida que també presta la FIJC. La base jurídica del tractament es basa en la preparació i execució d'un conveni a signar amb les persones que es beneficien d'aquest servei. Per tant, es basa en l'art. 6.1.b) RGPD. La informació sobre el tractament es proporciona als interessats en el mateix contracte, que tal com podem comprovar amb el document "*Convenio pisos acogida catalán*" aportat a aquesta auditoria, és correcte i ajustada a l'art. 13 RGPD.

  El procediment de selecció de les persones que han de rebre aquest servei requereix la implicació de Serveis Socials, amb qui l'entitat té un conveni. Són Serveis Socials els que elaboren un informe, fan una valoració sòcio-econòmica i, en definitiva, decideixen a qui es concedeix la prestació del servei. En general, l'assistent social fa una proposta i des de la FIJC s'ha de validar que la persona triada compleix els criteris del conveni. La FIJC es queda còpia de l'informe amb la valoració sòcio-econòmica.

  Caldria fer una reflexió en aquest apartat sobre la proporcionalitat i necessitat de disposar de determinada informació sobre les persones que, en relació a la prestació del servei de pisos d'acollida, pot resultar desproporcionada i innecessària.

- **Personal:**

  La base jurídica i de licitud del tractament consisteix en la preparació i execució d'un contracte de treball, de conformitat amb l'article 6.1.b) RGPD. La finalitat del tractament és la gestió i manteniment de la relació laboral.

  En aquests moments l'entitat està valorant si optar per un sistema de control horari del treballador a través d'empremta dactilar. Es fa notar que, a efectes de protecció de dades, aquesta forma de control requeriria una prèvia avaluació d'impacte, tal i com indica l'APDCAT.

  Segons les informacions proporcionades, molts dels serveis que realitza l'entitat es gestionen habitualment a través d'empreses subcontractades. Això fa també que la majoria de la plantilla sigui estable i no hi hagi un procediment previst de recepció de currículums o de selecció de personal que sigui habitual.

  En general, quan una persona entra a treballar a FIJC, s'aplica un procés d'acollida que implica proporcionar i fer signar, entre d'altres, els següents documents relatius a protecció de dades:

    - Informació al treballadors sobre protecció de dades (d'acord amb art. 13 RGPD) i compromís de seguretat.

    - Codi de Conducta de Seguretat de la Informació (document titulat "*DF-033_Codi_Conducta_Seguretat_Informaciov1*")

  Aquests documents han estat aportats per l'entitat a aquesta auditoria i, després de revisar-los, concloem que en general són correctes i que han estat degudament actualitzats i adaptats al RGPD.

D'acord amb les informacions i evidències proporcionades per l'entitat durant els treballs de camp, es va realitzar una acció d'enviar a tot el personal de l'entitat el Codi de Conducta de Seguretat de la Informació a través de la intranet, de manera que l'aplicació permet tenir constància de qui ha rebut i llegit efectivament el document. També es va realitzar un document a tot el personal per a recollir el seu consentiment per a l'ús de la imatge a la web corporativa. En aquest sentit, hi ha tres persones que van decidir no autoritzar l'entitat, i ara com ara la seva imatge personal no apareix a la web.

No consta que l'entitat faci un ús del correu electrònic personal de les persones treballadores o qualsevol altra dada que se situï més enllà de la relació laboral, llevat que calgui realitzar alguna comunicació puntual i esporàdica. En aquest sentit, no es detecten tractaments que puguin tenir la condició de desproporcionats o innecessaris des del punt de vista de la gestió de la relació laboral.

- **Gestió econòmica REDMO**

En aquest cas, la base jurídica es fonamenta en la gestió en el compliment d'un contracte o en l'aplicació de mesures precontractuals, segons l'art. 6.1.b) RGPD, i la finalitat és la facturació de les gestions realitzades per la FIJC en relació als transplantaments. Per tant, les poques dades personals que implica tractar són les mínimes per a la identificació del servei, com ara el nom del pacient i el codi del donant, entre d'altres. Atès que la informació sobre els tractaments ja s'ha donat prèviament, no caldria tornar-lo a donar als interessats. En la mesura del que sigui possible, s'hauria de procurar que les factures incloguessin dades seudonimitzades (sense identificar persones, sinó només codis), ja que la identificació de les persones resulta innecessària en la facturació de serveis a assegurances o a administracions públiques.

- **Donants econòmics / Socis / Iniciatives solidàries / Blanqueig de capitals**

La diferència entre donants i socis es basa en la contribució econòmica que fan. Mentre els donants econòmics fan aportacions puntuals, els socis contribueixen a través de quotes periòdiques. En el cas de les iniciatives solidàries, a qui l'entitat dona suport, les dades que en té l'entitat són de perfils assimilables als donants econòmics i socis. En qualsevol cas, els interessats reben cartes d'agraïment signades pel Sr. Josep Carreras, i en el cas dels socis reben també la revista "Imparables" tres cops l'any, a més de la memòria i d'altres informacions d'interès. La finalitat del tractament, en tots dos casos, és la gestió de les aportacions que realitzen i el manteniment d'una bona relació i comunicació.

En el cas del blanqueig de capitals, les dades es conserven en compliment d'una obligació legal com a base jurídica i per a la mateixa finalitat de donar compliment a aquesta obligació. En tot cas, les dades d'aquest tractament són les de socis i donants.

La base jurídica identificada per al tractament de les dades dels socis és el compliment d'un contracte (art. 6.1.b) RGPD), mentre que per als donants és la prestació del consentiment. (art. 6.1.a) RGPD).

La via principal per a fer-se socis o donants són els formularis que hi ha a la web. Tal com podem comprovar, en tots dos formularis ja hi ha una informació sobre el tractament de les dades. Aquesta informació no és completa (hi falta la referència a la DPD, per exemple),

però conté un enllaç a la pàgina "*Condicions generals d'ús*", que ja inclou una informació completa i ajustada a l'art. 13 RGPD.

Les dades també poden provenir de les empreses subcontractades que fan tasques de difusió al carrer i telemarketing. En aquests casos, però, es proporciona la informació sobre l'art. 13 RGPD en el moment de recollir les dades de forma correcta.

No consta un ús desproporcionat o il·lícit en relació a aquests tractaments.

- **Possibles / Testimonis / Participants en activitats de la FIJC**

Les dades corresponents a aquests tractaments corresponen a persones que manifesten interès en rebre informació sobre l'entitat i/o participen eventualment en activitats que organitza per a la difusió de les seves activitats. I aquesta és precisament la finalitat d'aquests tractaments: fomentar el coneixement sobre les activitats de FIJC. En tots tres casos, la base jurídica principal és el consentiment de l'interessat, que pot manifestar participar en una determinada activitat o voler rebre informació.

En general, d'acord amb les informacions proporcionades, hi ha procediments específics per a la recollida i gestió de les dades corresponents a aquests tractaments o per a la manifestació d'un consentiment. Així, els esdeveniments s'organitzen a través de formularis que, com es pot comprovar, ja inclouen una informació legal de conformitat amb l'art. 13 RGPD. En aquests formularis ja s'inclou una opció per a subscriure's expressament a una *newsletter*.

A la web hi ha un formulari titulat "*Vull estar al dia de la lluita contra la leucèmia*" en què també ja hi ha una informació legal sobre el tractament que és ajustada a l'art. 13 RGPD.

Es constata amb les responsables de l'àrea de comunicació que, tant a la revista "Imparables" com en xarxes socials, es publiquen de vegades fotografies sense que se n'hagi obtingut prèviament un consentiment exprés o s'hagi informat als actes públics sobre el fet de fer-s'hi fotos i publicar-les.

Recomanem disposar d'un model de document de consentiment exprés per a la publicació d'imatge, que s'hauria de fer servir sempre que s'hagi d'obtenir la imatge d'algú i publicar-la en mitjans de comunicació de l'entitat. No és vàlid el consentiment prestat oralment, sinó que s'ha d'obtenir sempre el consentiment exprés i per escrit de la persona interessada.

Recomanem que en els formularis d'inscripció als esdeveniment s'hi inclogui un avís sobre el fet que s'hi faran fotos i se'n farà difusió a través dels mitjans de comunicació de FIJC, i s'ofereixi la possibilitat de manifestar de forma expressa que no s'autoritza la realització de fotos.

- **Clients i proveïdors / Botiga online**

En aquest cas, les dades de clients i proveïdors, també les que provenen de la botiga online, responen a la finalitat de gestionar una relació comercial. La base jurídica del tractament és l'execució d'un contracte, segons l'art. 6.1.b) RGPD.

Comprovem que en el procés de realització d'una compra a la botiga online, l'aplicació demana crear un compte i informa sobre la seva política de privacitat, que l'usuari accepta tàcitament en proporcionar les dades. Aquesta política de privacitat, accessible a través d'un enllaç, ja conté les previsions sobre l'art. 13 RGPD. Recomanem, en tot cas, que la informació més bàsica sobre l'art. 13 RGPD sigui visible a la mateixa pàgina del formulari de recollida de dades (no només a través de l'enllaç), i que la informació completa sigui accessible igualment a través de l'enllaç. D'altra banda, recomanem revisar la informació que es proporciona actualment, per tal que sigui més ajustada a la finalitat de la botiga online.

D'altra banda, si en algun moment l'entitat disposa efectivament de dades de caràcter personal de clients i proveïdors que no són de la botiga online de forma habitual, caldrà tenir present la necessitat d'implementar procediments per a proporcionar la informació de l'art. 13 RGPD.

- **Aliances corporatives:**

Aquesta activitat de tractament fa referència a dades de persones físiques de què pot disposar l'entitat en la seva relació amb altres entitats o organitzacions. Són dades de persones que signen els convenis en nom d'aquestes organitzacions o actuen com a representants o interlocutors seus. La finalitat d'aquest tractament seria, per tant, la gestió d'aquests contactes personals a fi d'aconseguir o mantenir la col·laboració d'altres organitzacions, i la base jurídica identificada és l'execució d'un contracte (art. 6.1.b RGPD). Cal tenir present que aquest tractament revesteix realment poca entitat i risc, ja que en molts casos les dades són molt bàsiques i temporals, o poden fins i tot restar excloses de l'àmbit de protecció del RGPD.

No consten procediments específics de recollida o registre d'aquestes dades, però recomanem tenir present que, en cas que s'implementi un procediment d'aquest tipus, caldrà incorporar-hi una forma de complir el deure d'informació de l'art. 13 RGPD.

## Àrees de millora

| | |
|---|---|
| ● | Vegeu els comentaris anteriors, especialment les parts subratllades, que són les que fan referència de forma més específica a les àrees de millora. |

### 5.7. DRETS DE LES PERSONES INTERESSADES

Base legal: Articles 13-23RGPD

**Situació actual**

L'entitat ja disposa dels models i ja té un protocol definit per a l'exercici dels drets de les persones interessades, com es pot comprovar en revisar els documents "*DF-037 rev.01 Guia drets dels Interessats*", "*DF-036 Procediment Drets dels Interessats*" i "*IMP-060 v.01 Drets Afectats*". Aquest darrer document és el que conté els diferents formularis per a l'exercici dels drets, aportats durant aquesta auditoria. Per tant, ja està previst a FIJC un procediment actualitzat i ajustat al RGPD per a l'exercici dels drets d'accés, rectificació, oposició, supressió, limitació del tractament i portabilitat de les dades.

En general, el contacte amb la DPD per a l'exercici d'un dret es fa a través de la web o per correu electrònic. De vegades, però, el contacte es fa directament amb el REDMO, i són els responsables d'aquest registre els que després ho reenvien a la DPD.

D'acord amb les informacions proporcionades, ja hi ha hagut exercici de drets durant el darrer any per part de persones interessades. En concret, s'han exercit drets de rectificació i supressió, que s'haurien resolt en temps i forma.

**No detectada**

| | |
|---|---|
| ▲ | |

## 5.8. NOTIFICACIONS DE VIOLACIONS DE SEGURETAT

Base legal: Articles 24 i 33 RGPD

### Situació actual

L'entitat aporta evidències que acrediten l'existència d'un registre d'incidències i un protocol de notificació de violacions de seguretat. En concret, el document "*DF-035 rev.01 Procediment Violacions de seguretat de Dades Personals*" conté el protocol que descriu els processos relatius a incidències de seguretat, mentre que el document "*IMP-057 v1 Formulari notificació incidència seguretat interessat*" conté un model de comunicació que es faria servir per a notificar una violació de seguretat a les persones afectades. L'entitat també disposa d'un "*Formulario notificación brechas de seguridad AEPD*", que és el model de l'AEPD per a comunicar violacions de seguretat a l'autoritat de control.

Segons la informació i documentació analitzada, tot el personal té obligació de comunicar i registrar qualsevol incidència sobre seguretat en el tractament de les dades per correu electrònic o per qualsevol altre mitjà a la DPD de l'entitat, especialment el personal de l'àrea d'informàtica, que és més procliu a tenir coneixement d'incidències de seguretat.

D'acord amb el protocol de FIJC, és la DPD qui té atribuïdes les funcions de registre i gestió notificacions de violacions de seguretat, tant a l'autoritat de control com, si és el cas, també a la persona afectada. La decisió sobre la qualificació i gravetat de la incidència i la necessitat de dur a terme les accions de notificació, tanmateix, correspon al responsable del tractament i a la figura del Gerent. En qualsevol cas, la DPD, d'acord amb el protocol, hauria de registrar les raons d'aquestes decisions.

Comprovem que el Codi de Conducta de Seguretat de la Informació que s'ha proporcionat i es proporciona als treballadors en incorporar-se a l'entitat (el document "*DF-033_Codi_Conducta_Seguretat_Informaciov1*") no preveu l'obligació de comunicar al DPD qualsevol incidència detectada que pugui afectar a la seguretat de les dades. És possible que el personal hagi rebut aquesta instrucció en els cursos sobre protecció de dades que proporciona l'entitat, però no consta en la documentació inicial ni en d'altres comunicacions que s'hagin pogut comprovar.

El protocol "*DF-035 rev.01 Procediment Violacions de seguretat de Dades Personals*", esmentat més amunt, estableix la necessitat de comunicar a la DPD qualsevol incidència de seguretat com a una obligació dels treballadors, l'incompliment de la qual pot derivar en responsabilitats disciplinàries (inclosa la rescissió de contracte laboral) i d'altre tipus. No obstant, no consta que aquest document s'hagi proporcionat als treballadors.

D'acord amb les informacions proporcionades, no hi ha hagut encara cap notificació de violació de seguretat. En tot cas, sí hi ha hagut incidències, que, en ser detectades i registrades, han facilitat esmenar i reconduir determinades situacions de risc.

Durant els treballs de camp, a través de les entrevistes amb els diferents professionals, no resulta totalment clar que tot el personal actuaria de la mateixa manera, seguint un únic procediment d'actuació, en cas d'incidència o violació de seguretat. Això planteja el risc que l'entitat no actuï de forma adequada i no compleixi la seva obligació de comunicar qualsevol violació de seguretat que detecti a l'autoritat de control en el termini de 72 hores d'ença del moment de tenir-ne coneixement, tal com és la seva obligació.

## Àrees de millora

| | |
|---|---|
| ● | Tot i que el procediment que ja preveu l'entitat és correcte, és possible millorar-lo a través d'accions que permetin que tot el personal sigui conscient de l'existència d'aquest procediment i de l'obligació de comunicar fuites de seguretat a la DPD. En especial, recomanem que aquesta obligació que té tot el personal de l'entitat s'incorpori al Codi de Conducta de Seguretat de la Informació en forma d'instrucció. |

### 5.9. DIFUSIÓ DE FUNCIONS I OBLIGACIONS

Base legal: Articles 24 i 25 RGPD

**Situació actual**

D'acord amb les evidències i informacions proporcionades, i tal com s'ha esmentat anteriorment en aquest informe, l'entitat ja ha realitzat accions suficients de difusió destinades a proporcionar instruccions als treballadors sobre les seves obligacions en matèria de protecció de dades i les mesures de seguretat aplicables. En particular, s'ha proporcionat (i està previst que es proporcioni a tot el personal que es vagi incorporant) un Codi de Conducta de Seguretat de la Informació. Aquest document presenta un contingut correcte sobre les obligacions del personal en el tractament de les dades i l'aplicació de mesures de seguretat, però no inclou cap referència al procediment de notificació d'incidències i violacions de seguretat.

D'altra banda, dins aquesta tasca de difusió que correspon a la DPD, consten suficients evidències d'haver-se realitzat activitats de formació en matèria de protecció de dades destinades al personal.

**No detectada**

| | |
|---|---|
| ▲ | Malgrat que les evidències proporcionades deixen suficient constància d'haver-se realitzat una correcta activitat de difusió i formació, és possible millorar el Codi de Conducta de Seguretat de la Informació amb una instrucció específica sobre l'obligació que té tot el personal vinculat a FIJC de posar en coneixement de la DPD qualsevol incidència en la seguretat de les dades de forma immediata, tal com hem comentat en el punt anterior. |

## II – BLOC MESURES DE SEGURETAT

### 5.10. DILIGÈNCIA DELS ACCESSOS

**L'establiment del control de l'accés de persones autoritzades a les dades personals: evitar pantalles desateses, documents en zones d'accés públic, etc. Cal procedir a bloquejar el dispositiu o bloquejar la sessió en absentar-se del lloc de treball.**

**Situació actual**

De forma generalitzada, tal com hem pogut comprovar durant els treballs de camp, tots els espais, magatzems, despatxos i àrees de l'entitat que contenen o guarden documentació amb dades de caràcter personal disposen de sistemes de tancament, de manera que la informació es guarda de forma segura i fora de l'abast d'usuaris no autoritzats. Els treballadors coneixen la seva obligació de tancar les sales i despatxos que continguin informació confidencial, quan ja no es fan servir o quan acaba la jornada laboral.

Les instal·lacions de FIJC, que consisteixen en dues plantes d'un mateix edifici, disposen d'un sistema d'alarma. La primera persona que entra a l'oficina ha de desconnectar l'alarma introduint-hi un codi, per a la qual cosa disposarà de tres intents. Després de tres intents fallits, l'empresa de seguretat que gestiona l'alarma trucarà per a comprovar si hi ha un problema de seguretat i demanar la clau que desactiva l'alarma.

Tal com podem comprovar durant els treballs de camp, la sala de servidors es troba tancada amb clau fora de la jornada laboral, i només és accessible amb clau per part de personal.

El document Codi de Conducta de Seguretat de la Informació que es proporciona a tot el personal ja conté instruccions de seguretat sobre la importància i l'obligació protegir els espais de treball i els accessos a les dades. D'una banda, també conté instruccions sobre la confidencialitat que cal mantenir respecte a les dades personals a què pot tenir accés el personal com a conseqüència de les seves responsabilitats. També recorda la necessitat d'accedir sempre als entorns de tractament de dades a través de contrasenya, que haurà de modificar-se anualment, a més de tenir en consideració mesures de seguretat. D'altra banda, el Codi de Conducta també preveu polítiques de taula neta i pantalla neta, les quals estan destinades a evitar precisament accessos indeguts. No cal dir que la política de pantalla neta preveu que l'usuari, en absentar-se del seu lloc de treball, activi el protector de pantalla. De tota manera, en cas d'una absència perllongada de més de 30 minuts, el protector de pantalla s'activa automàticament.

**No detectada**

| | |
|---|---|
| ▲ | |

### 5.11. EMMAGATZEMATGE EN SUPORT PAPER

**Els documents en paper i suports electrònics s'emmagatzemaran en lloc segur (armaris, calaixos o estances d'accés restringit).**

**Situació actual**

En general, tota la documentació es troba desada en carpetes, calaixos i armaris, generalment sota clau i amb accés restringit als responsables del seu tractament autoritzat.

Els espais i despatxos en què es guarda documentació en paper es troben generalment tancats amb clau o restringits per un control d'accés per targeta, com és el cas també dels accessos a les instal·lacions. Tal com hem indicat en el punt precedent, les zones d'arxiu estan degudament restringides, i només són accessibles sota clau per part de personal autoritzat.

No es constata durant els treballs de camp l'existència de documentació que no es trobi degudament desada o custodiada.

**No detectada**

| | |
|---|---|
| ▲ | |

## 5.12. DESTRUCCIÓ DE SUPORTS

**No es llençaran documents o suports electrònics amb dades personals sense garantir-ne la destrucció.**

**Situació actual**

Pel que fa a la documentació en paper, tal com podem comprovar personalment durant els treballs de camp, l'entitat disposa de trituradores i contenidors per a la destrucció segura en gairebé totes les seves àrees. És en aquests contenidors on es diposita la documentació sensible o confidencial per a la seva eliminació segura.

Segons el Document de Seguretat TIC, FIJC té contractada una empresa de destrucció segura (anomenada ECOLOGIC) que recull el contingut dels contenidors, aplica mesures de destrucció i emet certificats que l'eliminació s'ha dut a terme. De forma periòdica i a requeriment de l'entitat, la citada empresa externa recull el contingut dels contenidors, de la qual cosa se'n deixa constància documental.

D'acord amb les previsions del Codi de Conducta de Seguretat de la Informació, els documents inservibles que continguin informació confidencial s'han de destruir mitjançant una trituradora de documents o servei de destrucció segura.

Pel que fa a la destrucció de suports electrònics que contenen dades de caràcter personal, el Codi de Conducta de la Seguretat de la Informació ja preveu que tots els dispositius que continguin informació sensible i/o dades personals de categories especials i ja no es facin servir siguin destruïts mitjançant un sistema de destrucció de dades certificat i segur, a fi de prevenir una possible recuperació de la informació. L'entitat té contractada una empresa especialitzada, que pot dur a terme processos de destrucció segura de suports i dispositius. El Document de Seguretat TIC preveu que la destrucció dels suports electrònics, un cop formatats, els faci l'empresa Leinad a través d'un procés de premsat hidràulic.

**No detectada**

| | |
|---|---|
| ▲ | |

## 5.13. CRITERIS D'ARXIU

**S'establiran criteris d'arxiu per a la documentació que contingui dades de caràcter personal, i es custodiarà de forma adequada quan no s'utilitzi aquesta documentació.**

### Situació actual

En general, els arxius en suport paper han de permetre garantir la correcta conservació de la documentació, la localització i consulta de la informació, i fer possible l'exercici dels drets dels interessats respecte a l'accés, oposició, supressió, rectificació, limitació i portabilitat sobre les seves dades personals.

A FIJC, en general es guarda molt poca documentació en paper, però aquesta es troba desada i conservada de forma segura en diferents àrees, segons l'ús i disposició que en fan els professionals, d'acord amb les diferents tasques i responsabilitats laborals. Vegem ara les àrees en què es pot conservar més documentació en paper:

REDMO (documentació de donants i pacients): En general, tota la documentació en paper que es fa servir té un caràcter temporal i acaba, en molts casos, essent destruïda, cosa que sol passar després de desar-la electrònicament a través del programa DOCUWARE. No obstant, per a emmagatzemar la documentació en paper l'entitat té subcontractat un servei de custòdia amb una empresa especialitzada. Aquesta empresa té un magatzem dedicat a El Prat de Llobregat en condicions de seguretat, on està desada la documentació en paper que té més de 10 anys (prèvia al tractament informatitzat).

No s'han iniciat procediments de destrucció sistemàtica de documentació més antiga. En tot cas, per si s'hagués de localitzar i recuperar documentació emmagatzemada antiga, ja es guarden llistats amb tota la documentació ben classificada.

Pisos d'acollida: Aquest servei implica tractar diferent informació de caràcter sensible, com ara els contractes i els informes de caràcter sòcio-econòmic que elaboren els serveis socials sobre les famílies. En tot cas, aquesta documentació en paper sempre acaba destruïda, si bé es conserva de forma escanejada de manera indefinida.

Recursos Humans: D'acord amb les informacions proporcionades, tota la gestió la realitza una empresa subcontractada, que envia les nòmines per correu electrònic als treballadors. En qualsevol cas, l'entitat pot conservar documentació de recursos humans de forma indefinida en suport paper, desada en armaris i calaixos, de forma organitzada.

A les àrees de comunicació i màrqueting, fidelització i iniciatives solidàries, no consta una gestió destacable en suport paper, ja que tots els processos es vehiculen a través d'aplicacions informàtiques.

### Àrees de millora

| | |
|---|---|
| ● | Cal establir terminis i criteris de destrucció de la documentació més antiga i innecessària, ja que es corre el risc que la informació o documentació que conté dades de caràcter personal es conservi durant més temps del que sigui necessari i això sigui, per tant, un tractament indegut. Cal que l'entitat estableixi criteris i |

| | |
|---|---|
| | terminis legals de conservació més clars al registre d'activitats de tractament i que procedeixi a l'eliminació de documentació antiga i innecessària.<br><br>Pot ser recomanable tenir en compte els protocols de referència de la Comissió Tècnica de Documentació Clínica sobre terminis de custòdia documental. |

### 5.14. REGISTRE D'ACCESSOS DOCUMENTAL

**Categories especials de dades: es restringirà l'accés a aquest tipus de documentació, s'habilitaran mètodes per a la seva destrucció i es durà a terme un registre d'accés a aquests documents.**

**Situació actual**

D'acord amb les informacions proporcionades, la documentació en suport que paper que encara es fa servir a l'entitat, es troba generalment desada als seus corresponents despatxos, que es troben tancats en clau, quan no es fan servir.

Pel que fa a la documentació més antiga, que es troba desada en un magatzem a El Prat de Llobregat sota la custòdia d'una empresa especialitzada, ja hi ha un control i registre de tota la documentació, i està previst un procediment per a la seva recuperació, en cas necessari. El procediment implica tenir en tot moment un coneixement de la ubicació de la documentació i de la persona que la pot haver sol·licitat i està pendent de retornar-la.

L'entitat ja té mitjans per a la destrucció de documentació confidencial, como ara destructores de paper i contenidors per a la destrucció segura, que gestiona una empresa subcontractada. Aquests darrers són proporcionats per una empresa especialitzada, amb qui FIJC ha contractat la prestació d'aquest servei.

**No detectada**

| | |
|---|---|
| ▲ | Malgrat que s'apliquen correctament mesures de registre d'accessos, recomanem tenir en compte els protocols de la Comissió Tècnica de Documentació Clínica sobre destrucció i translació a d'altres suports:<br><br>http://aquas.gencat.cat/ca/ambits/projectes/CTMDC/criteris-protocols/ |

## 5.15. IDENTIFRICACIÓ I AUTENTICACIÓ

**S'establiran mecanismes d'autenticació personalitzats per accedir als sistemes mitjançant, per exemple, un usuari i contrasenya específic per a cada treballador (identificació inequívoca).**

**La contrasenya tindrà almenys 8 caràcters (números i lletres) i l'empresa decidirà la complexitat d'aquestes claus. Es canviaran les contrasenyes, com a mínim, un cop l'any.**

**Situació actual**

D'acord amb les informacions proporcionades i la documentació aportada, tots els usuaris ja estan identificats i registrats, i ja hi ha un control sobre el nivell d'accés autoritzat que pot tenir cadascú.

El document "*Registre usuaris*" conté una relació actualitzada dels usuaris autoritzats a accedir als diferents entorns informàtics.

En general, el procediment d'alta d'un nou usuari comença quan des de la persona responsable del departament o àrea es realitza una petició a sistemes informàtics i s'informa sobre les funcions que realitzarà el nou usuari i el perfil d'accés que ha de tenir. Els responsables de sistemes informàtics apliquen el perfil d'accés que correspongui d'acord amb les funcions atribuïdes.

Per a la primera alta al directori actiu, des de recursos humans es facilita a l'usuari un nom d'usuari i una contrasenya, que pot canviar voluntàriament. Com que gran part del sistema està centralitzat, ja es propaga el nom d'accés i la contrasenya a tots els altres sistemes i aplicacions a què l'usuari hagi de tenir accés.

El nom d'usuari consisteix habitualment en la inicial del nom i el cognom; en el cas del DOCUWARE, que es fa servir per a la gestió documental, el nom d'usuari és excepcionalment el nom de la persona (sense cognom).

La contrasenya ha de contenir sempre un mínim de 7 caràcters i ser robusta (ha d'incloure majúscules, minúscules, i caràcters no alfanumèrics, i no pot ser una repetició d'alguna de les 24 contrasenyes anteriors). La contrasenya s'ha de renovar necessàriament cada 180 dies. En el cas del DOCUWARE, la contrasenya no es canvia mai obligatòriament.

El criteri que s'aplica és que qualsevol aplicació es pugui integrar al directori i es pugui adaptar a la gestió d'usuari i contrasenya de l'entitat. Tots els entorns segueixen la mateixa política, llevat de comptades excepcions, com ara el programa DOCUWARE, com ja hem comentat.

En tot cas, s'apliquen mesures de seguretat en el control d'accés, la limitació per intents d'accés fallits (que són 10 en el Directori actiu) i el bloqueig per inactivitat de la sessió, que, en la seva aplicació al Windows, s'activa al cap de 15 minuts. En el cas del DOCUWARE, també hi ha una mesura d'intents d'accés fallits (limitats, en aquest cas, a 3), bloqueig i registre de tots els accessos i intents d'accés.

**No detectada**

| | |
|---|---|
| ▲ | |

### 5.16. PERFILS

**S'establiran perfils d'usuaris amb diferents nivells d'accés a dades personals segons les funcions del treballador; Quan un dispositiu s'utilitzi per al tractament de dades personals i fins d'ús personal es recomana establir perfils diferents. Es recomana disposar de perfils amb drets d'administració per a la instal·lació i configuració del sistema i usuaris sense privilegis.**

**Situació actual**

D'acord amb les informacions i evidències proporcionades, hi ha diferents entorns informàtics de tractament de dades, i entre ells destaca particularment el REDMO, que es fa servir per a la gestió dels processos de selecció de donants en relació a un pacient i conté dades de categoria especial. Aquest programa ja permet configurar diferents tipus d'accés, configurant especialment dos espais separats, que són l'àrea de pacients i l'àrea de donants, que es corresponen amb dues àrees de treball diferenciades i reflecteixen aquesta separació tècnica i funcional entre elles. D'aquesta manera, els usuaris del REDMO que treballen amb donants no tenen accés a dades de pacients, i a la inversa, i això és així, si més no, de forma generalitzada (hi ha algunes excepcions, que poden ser objecte de millora, com podem veure en d'altres apartats d'aquest informe).

En general, en funció de les responsabilitats laborals atribuïdes a cada persona dins l'entitat, ja hi ha diferents perfils d'accés a entorns informatitzats, aplicacions i dades de caràcter personal. Així, per exemple, el personal vinculat a la gestió de socis i les seves donacions econòmiques, tindrà accés al programa EPISOCIS, mentre que el personal adscrit a l'àrea de donants, tindrà accés al REDMO, però també, segons les seves responsabilitats laborals, al programa EPIDONOR (gestió de petició de proves a donants) o a l'EMDIS (peticions de proves des de l'estranger). Tots els usuaris del REDMO tenen també accés al DOCUWARE CLOUD, on es desa habitualment tota la documentació vinculada a les gestions del REDMO.

En general, Document de Seguretat TIC ja descriu detalladament els diferents entorns informàtics que es fan servir habitualment a FIJC per al tractament de les dades i el tipus de servei i professionals que hi tenen accés.

L'accés al correu electrònic es troba implícit en el procediment d'accés general al domini FIJC.

**No detectada**

| | |
|---|---|
| ▲ | |

### 5.17. MANTENIMENT DE LES XARXES

**Els dispositius i ordinadors utilitzats per a la conservació i el tractament de les dades personals hauran de mantenir-se actualitzats. En aquests dispositius es disposarà d'un sistema d'antivirus instal·lat i degudament actualitzat.**

**Situació actual**

Tots els recursos i sistemes utilitzats a FIJC per al tractament de les dades es troben degudament actualitzats.

Els servidors físics es troben en una sala de l'entitat, i dins s'hi troben els servidors virtuals. En aquest sentit, totes les bases de dades es troben a la casa. Per al REDMO, tanmateix, es fa servir un software anomenat DOCUWARE, que es troba al núvol.

Com a entorns de tractament més habituals, es fan servir dos programes CRMs fets a mida anomenats EPIDONOR (gestió de donats i pacients) i EPISOCIS (gestió de persones que fan donacions econòmiques).

Per a la connexió a internet es fa servir un Firewall per hardware instal·lat entre els servidors de Hyper-V i internet, que filtra les entrades i sortides d'informació, segons la configuració de seguretat, i està destinat a evitar possibles atacs que es produeixin des d'internet.

Com a mesura de seguretat, l'entitat té instal·lats i actualitzats dos tipus d'antivirus, un per als servidors i un altres per a les estacions de treball, segons està explicat al Document de Seguretat TIC. Als servidors s'utilitza Microsoft Windows Defender, que ajuda a detectar software malintencionats o no detectats i fa servir un sistema de protecció en temps real per a analitzar tot el que es descarrega o executa als dispositius. D'altra banda, a les estacions de treball hi ha instal·lat l'antivirus Symantec Endpoint Protection versió 14. És una protecció per a punts finals de diverses capes que permet detectar amenaces conegudes, desconegudes i de "dia zero". El document "Data Sheet Endpoint Security" explica els processos de seguretat que depenen de l'ús de Symantec Endpoint Protecion com a antivirus instal·lat als diferents equips.

**No detectada**

| | |
|---|---|
| ▲ | |

## 5.18. ACCESOS REMOTS

**Per evitar accessos remots indeguts a les dades personals es prendran les mesures corresponents com l'existència de Firewall.**

**Situació actual**

Tot i que la norma general és que totes les aplicacions s'han de fer servir únicament des de les instal·lacions de FIJC, l'entitat permet a determinats usuaris, per raons justificades de les seves responsabilitats laborals, que accedeixin remotament als sistemes. Es tracta d'un accés excepcional i ha d'estar justificat.

L'accés remot es fa a través de VPN i permet un accés a l'escriptori. Per a aquest accés es fa servir el mateix nom d'usuari i contrasenya que es fa servir per a accedir al directori actiu.

Els usuaris autoritzats són el Gerent, el Director del REDMO i el responsable de Sistemes de l'entitat. No consten, però, com a tal ni al Document de Seguretat TIC

D'altra banda, el sistema està proveït d'un Firewall ubicat al servidor, que ja preveu el filtratge de totes les entrades i sortides de telecomunicacions per motius de seguretat.

**No detectada**

| | |
|---|---|
| ▲ | Seria convenient que els usuaris autoritzats a accedir remotament constessin expressament com a tal o bé al document Excel "*Registre usuaris*" o bé al Document de Seguretat TIC en l'apartat d'accessos remots. |

## 5.19. CÒPIES DE SEGURETAT

**Periòdicament (mínim setmanal) es duran a terme processos de còpia de seguretat de les dades personals en un suport diferent al que s'utilitza pel treball diari. Es disposarà d'una còpia de seguretat en un lloc diferent d'on s'emmagatzemen les dades.**

### Situació actual

El Document de Seguretat TIC que s'ha aportat a aquesta auditoria ja conté les característiques tècniques dels procediments aplicats en la realització de còpies de seguretat dels diferents servidors de l'entitat. Aquest mateix document també descriu les mesures de revisió adoptades per l'entitat.

Segons el Document de Seguretat TIC, les màquines virtuals que es fan servir a FIJC per al tractament de les dades estan replicades sempre en un altre dels servidors Hyper-V. D'aquesta manera, sempre és possible canviar d'un servidor a un altre i utilitzar les rèpliques en cas que caigués un servidor Hyper-V. Les rèpliques, a més, posseeixen molts punts de còpies, que es van fent durant tot el dia, de manera que és possible restaurar en qualsevol moment una màquina virtual a l'últim punt replicat (generalment, pocs minuts o segons abans) o recuperar fins i tot punts anteriors a les últimes 24 hores. D'altra banda, les màquines virtuals són exportades periòdicament a un servidor local de fitxers com a còpia de seguretat completa de servidor virtualitzat. Aquestes còpies es realitzen mensualment.

Pel que fa al núvol privat (local) hi ha un servidor de còpies de seguretat (DPM) que centralitza i gestiona tot el sistema de còpies de seguretat i restauracions. En concret, fa còpies dels fitxers allotjats al servidor DFS i de les bases de dades SQL. Les còpies de seguretat tenen una periodicitat que varia dels 15 als 60 minuts com a mínim, i es fan en un sistema de discs al DPM local, a fi d'assegurar una ràpida recuperació. En paral·lel, però, també es fan còpies al núvol de Microsoft Azure a fi d'assegurar la còpia en un lloc segur i extern a la FIJC.

Les retencions de les còpies varien des de retencions de totes les còpies diàries durant un mes a retencions de còpies anuals de fins a 10 o 20 anys. Hi polítiques de retencions diàries, setmanals, mensuals i anuals. El sistema permet la recuperació de gran quantitat de punts de recuperació. D'altra banda, les còpies al núvol públic de Microsoft Azure, situades fora de la FIJC, tenen normes de retenció de 180 dies, de 104 setmanes, de 60 mesos i de 15 anys, amb la possibilitat d'augmentar-les a 20 anys.

Hi ha una previsió específica per a permetre la recuperació, en cas de pèrdua parcial del núvol privat, inclòs el servidor DPM. Una màquina virtual de reserva permetria la recuperació de qualsevol còpia a Azure de manera àgil.

No consta que hi hagi un procediment de revisió dels diferents processos de còpia de seguretat.

### Àrees de millora

| | |
|---|---|
| ● | Tot i que els procediments de còpia descrit són correctes, com a aspecte millorable, caldria implementar un procediment de revisió d'aquests procediments (per exemple, cada 6 mesos) i documentar-ne el resultat. |

## 5.20. REGISTRE D'ACCESSOS INFORMÀTICS

**Categories especials de dades: es durà a terme un registre d'accessos d'aquest tipus de dades.**

### Situació actual

Segons les informacions proporcionades, ja hi ha un registre de tots els accessos als entorns EPISOCIS, EPIDONOR i DOCUWARE, que són els entorns que poden contenir dades de categoria especial (per exemple, dades de salut). D'acord amb aquesta mesura de seguretat, cal verificar que la implementació d'un registre d'accessos permet que es guardi efectivament, de cada intent d'accés a les dades de salut, com a mínim, la identificació de l'usuari, la data i hora de l'accés a les dades de salut, la informació accedida, el tipus d'accés i si aquest ha estat autoritzat o denegat. En relació a accessos autoritzats, caldria guardar la informació que permetés identificar el registre accedit, tenint en compte que el període mínim de conservació de les dades enregistrades ha de ser de 2 anys.

El Document de Seguretat TIC de l'entitat preveu l'existència d'un servidor exclusiu per a controlar i monitoritzar possibles accessos indeguts que puguin realitzar-se des de l'exterior. No obstant, no consta documentalment l'existència d'un procés de revisió d'accessos indeguts que es realitzi sobre els accessos que fan els usuaris autoritzats. No hi ha evidència tampoc de revisions d'accessos indeguts que s'hagin fet anteriorment.

### Àrees de millora

| | |
|---|---|
| ● | Segons les informacions proporcionades i el Document de Seguretat TIC, l'entitat ja realitzaria un registre d'accessos i un control informal de possibles accessos indeguts, però caldria formalitzar i definir aquest procediment. No hi ha tanmateix cap evidència documental d'aquest procediment.<br><br>Com a procediment, es podria establir la realització d'una revisió mensual, fent una selecció a l'atzar de registres i dates, i documentar de forma convenient per part de la DPD la detecció o no de possibles accessos indeguts. Els registres i dates que podrien ser objecte de la revisió podrien triar-se a l'atzar, o tenir en compte criteris de risc d'accés indegut (casos en què donants o pacients siguin familiars de persones treballadores, VIPs, etc.). |

### 5.21. INVENTARI

**Es disposarà d'un inventari actualitzat dels diferents suports/dispositius que continguin dades personals.**

**Situació actual**

Tots els suports i dispositius que es fan servir a FIJC per a tractar i conservar dades de caràcter personal ja estan degudament identificats i inventariats, i presenten un codi. L'entitat ja té inventariats els suports i dispositius, però no consten al Document de Seguretat TIC.

En general, segons informacions proporcionades, ja es preveu l'actualització i control dels inventaris de suports i dispositius informàtics.

**No detectada**

| | |
|---|---|
| ▲ | Caldria incloure l'inventari de suports i dispositius al Document de Seguretat TIC o en un seu annex, per tal de tenir-lo correctament documentat. |

## 5.22. SORTIDA DE DADES

**Categories especials de dades: quan calgui realitzar l'extracció de dades personals fora del recinte on es realitza el seu tractament, ja sigui per mitjans físics o electrònics, s'haurà de valorar la possibilitat d'utilitzar un mètode d'encriptació.**

### Situació actual

D'entrada, és important remarcar que, tal com estableix el Document de Seguretat TIC, les eines de comunicació que fa servir habitualment l'entitat per a comunicar-se amb altres registres de donants ja preveuen per defecte l'aplicació de mesures d'encriptació en totes les comunicacions. És el cas, per exemple, de l'EMDIS, que es fa servir per a la comunicació de dades entre registres i que també facilita que les comunicacions duguin signatures digitals GnuPG versió 2.0.30 (PGP). En el cas de les aplicacions web EPICdp i EpicSocisWebProeedores, que fan servir els proveïdors que gestionen les bases de dades, també està prevista l'aplicació de processos d'encriptació, tal com es pot comprovar al Document de Seguretat TIC.

El Codi de Conducta de Seguretat també preveu instruccions específiques sobre les comunicacions que incloguin dades de salut:

"*Punt 2.3.2: Si les dades s'han d'enviar fora de del REDMO, amb la finalitat de trobar un donant adequat per a un pacient que requereixi un trasplantament de progenitors hematopoètics, les dades mèdiques s'enviaran per correu electrònic mitjançant una plataforma de comunicació segura que permeti el xifratge i mai s'inclouran dades personals a l'assumpte o al text del correu electrònic*".

D'altra banda, segons les informacions proporcionades, si bé s'han donat instruccions al personal sobre la necessitat d'enviar els correus aplicant procediments d'encriptació, com a ara fent servir el WinZip, la realitat d'alguns interlocutors del sector sanitari (també internacionals) i la urgència de les acciones requerides fan molt difícil l'aplicació d'aquests procediments en tots els casos.

Pel que a suports o dispositius que continguin dades de caràcter personal, no consta que n'hi hagi sortides habituals des de les instal·lacions de FIJC, llevat d'alguns supòsits excepcionals, com és el cas dels tres mòbils de guàrdia, que estan perfectament identificats i registrats.

### Àrees de millora

| | |
|---|---|
| ● | Per tal de minimitzar el risc en el tractament de les dades, totes les comunicacions que continguin dades sensibles o de categoria especial (per exemple, dades de salut) no haurien d'enviar-se a través del correu electrònic ordinari, sinó aplicant mesures i procediments d'encriptació, sempre que sigui possible i això no suposi posar en perill la salut de les persones involucrades en els processos de donació. En aquest sentit, cal que l'entitat fomenti el desenvolupament de comunicacions segures amb els seus interlocutors i que només de forma justificada es plantegi fer servir formes de comunicacions poc segures, com ara el correu electrònic ordinari. |

## 5.23. CENTRE DE PROCESSAMENT DE DADES

**S'establiran mecanismes de restricció d'accés a la sala on es trobin els servidors (CPD).**

### Situació actual

Tal com podem comprovar durant els treballs de camp, la sala de servidors disposa de tancament mecanitzat i, fora de la jornada laboral, només és accessible amb clau per part de personal autoritzat (Gerent, responsable TIC i proveïdor informàtic extern). No obstant, està oberta durant la jornada laboral i podria ser accessible.

El CPD es troba dins un espai interior tancat i refrigerat, i està dotat amb un doble sistema de refrigeració i un mesurador de temperatura, el qual que, en cas de detectar una temperatura molt alta, dispararia una alarma. D'una banda, un armari rack conté pròpiament el servidor, mentre que un altre armari conté un equip de comunicacions IT.

Dos SAIS permetrien al CPD disposar d'un corrent alternatiu de trenta minuts aproximadament, per al cas d'interrupció del subministrament elèctric general.

No hi ha extintor dins la sala del servidor, però si al costat de l'entrada. En aquest sentit, el servidor es trobaria a l'abast, en cas d'incendi.

### Àrees de millora

| | |
|---|---|
| ● | Com a únic element de millora i amb la finalitat de minimitzar el risc d'accessos indeguts, cal que la sala de servidors estigui tancada no només fora de la jornada laboral, sinó sempre que no se'n faci cap ús, i també particularment dins la jornada laboral. |

### 5.24. EMMAGATZEMATGE DE FITXERS

**Com a norma general, els fitxers que continguin dades personal s'emmagatzemaran en un servidor de fitxers i no en els dispositius dels usuaris de forma local.**

**Situació actual**

Tant per les instruccions que dona l'entitat al seu personal, tal com es pot comprovar amb el Codi de Conducta de Seguretat de la Informació aportat a aquesta auditoria, com per les informacions proporcionades, hi ha una prohibició d'emmagatzemar dades de caràcter personal en els equips locals o dispositius.

El Codi de Conducta de Seguretat de la Informació estableix instruccions rellevants per al personal sobre emmagatzematge de dades en els dos punts següents:

Punt 2.3.2: "*El personal del REDMO només podrà descarregar dades mèdiques no anònimes dins de l'entorn segur de l'oficina del REDMO. No es permet la descàrrega o la transferència de dades que continguin identificadors semi anònims en ordinadors personals o domèstics (...).*"

Punt 4.2 "*No emmagatzemar còpies locals de fitxers que continguin dades personals en dispositius portàtils, ja siguin personals o REDMO*."

D'altra banda, tal estableix el punt 4.1 del citat document, els equips informàtics, telèfons mòbils, telèfons intel·ligents i targetes de memòria només poden treure's de l'entitat amb l'autorització expressa del responsable del tractament. Sense aquesta autorització, resta prohibit treure aquests dispositius de l'entitat.

**No detectada**

| | |
|---|---|
| ▲ | |

## 6. CONCLUSIONS

Després de realitzar totes les actuacions necessàries a les dependències de l'entitat, completar les entrevistes amb els corresponents responsables d'àrea, valorar la documentació aportada i avaluar els sistemes de tractament de la informació, l'equip auditor detecta que les àrees de millora i de no conformitat, d'acord amb la normativa vigent, són:

| ÀREES DE MILLORA |
|---|
| I – BLOC GENERAL |
| 5.2. Registre d'activitats de tractament.<br>5.3. Definició de les mesures de seguretat per part del responsable de tractament.<br>5.5. Encarregats del tractament i proveïdors sense accés a dades.<br>5.6. Licitud del tractament, base jurídica, informació i consentiment.<br>5.8. Notificacions de violacions de seguretat. |
| II – BLOC DE MESURES DE SEGURETAT |
| 5.13. Criteris d'arxiu.<br>5.19. Còpies de seguretat.<br>5.20. Registre d'accessos informàtics.<br>5.22. Sortida de dades.<br>5.23. Centre de processament de dades. |

Barcelona, 15 de novembre de 2019.

Pere Ruiz Espinós

- Soci -

Caterina Bartrons Pou

- Gerent -