Protecció de dades de caràcter personal

Juny de 2022
Protocol: C-14.419

Fundació Institut Guttmann

Informe d'Auditoria de Protecció de Dades de Caràcter Personal

Fundació Unió Carrer de València, 333 · 08009 Barcelona · Tel 93 209 36 99 · Fax 93 200 86 38
Faura-Casas Carrer Còrsega, 299 6ª · 08008 Barcelona · Tel 902 28 28 30 · Fax 93 302 65 96

INDEX

1. OBJECTIUS 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 Institut Guttmann
CIF	G08519100
Domicili	Camí de Can Ruti s/n 08916 Badalona

3.1.2. Descripció de l'activitat

La Fundació Institut Guttmann és una entitat privada d'iniciativa social, sense ànim de lucre i aconfessional, impulsada per la societat civil catalana, constituïda l'any 1962. El seu objectiu principal és promoure, impulsar i aconseguir la rehabilitació integral de les persones afectades per una lesió medul·lar, un dany cerebral adquirit o una altra discapacitat d'origen neurològic, desenvolupar la recerca i la docència en aquest àmbit de la neurociència i prestar-los el suport i els serveis més convenients per assolir una reinserció social satisfactòria.

En data de 18 de juny de 2014 s'aprovà la fusió per absorció de la Fundació Privada Institut de Neurorehabilitació Guttmann per la Fundació Institut Guttmann, que es va fer efectiva a partir de 2015. D'aquesta manera, totes les activitats de la Fundació Privada Institut de Neurorehabilitació Guttmann passen a integrar-se dins les activitats que ja duia a terme la Fundació Institut Guttmann, subrogant-se doncs en tots els drets i obligacions de l'entitat fusionada i extingida. Els serveis prestats per l'entitat són els d'hospitalització d'aguts, d'hospital de dia, neurorehabilitació, consultes externes, recerca i docència.

Les instal·lacions actuals de Fundació Institut Guttmann a Badalona són de 2002.

D'altra banda, el projecte Guttmann Barcelona als carrers Meridiana/Garcilaso de Barcelona, suposa l'existència d'unes noves instal·lacions, entre les quals hi ha un gimnàs, sales de tractament, consultes mèdiques (neuroclínica) i els apartaments Guttmann Barcelona Life domotitzats per a persones amb necessitats especials.

3.2. TREBALLS EFECTUATS

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

- Àrea del delegat de protecció de dades
- Àrea informàtica
- Àrea de recursos humans
- Àrea econòmica-financera

- Àrea de comunicació i de responsabilitat social corporativa
- Amics de l'Institut Guttmann.
- Àrea d'admissions
- Àrea d'atenció a l'usuari
- Àrea d'arxiu
- Àrea de rehabilitació funcional
- Àrea d'infermeria
- Àrea de neuropsicologia
- Àrea de direcció mèdica
- Infraestructures, Serveis i Medi Ambient (ISMA)
- Àrea de Videovigilància
- Àrea de recerca
- Àrea de treball social
- Àrea de voluntariat

3.2.1. Data de realització de l'auditoria

Data	20 i 21 de juny de 2022

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	Sr. Javier Remacha	Delegat de protecció de dades (DPD)
2	Sr. Roger Marsal	Cap de sistemes d'informació
3	Sra. Elisenda Bassas	Cap de recursos humans
4	Sr. Hèctor López	Cap de l'àrea econòmica-financera
5	Sra. Elisabet González	Cap de comunicació i de responsabilitat social corporativa
6	Sr. Sergi Pedraza	Cap d'admissions
7	Sr. Santi Vilà	Responsable d'arxiu
8	Dra. Narda Murillo	Cap de rehabilitació funcional
9	Sra. Eulàlia Castillo	Supervisora d'infermeria
10	Sra. Antònia Enseñat	Cap de Neuropsicologia
11	Dr. Cristian Figueroa	Subdirector mèdic
12	Sra. Sílvia Calvo	Cap de l'ISMA (Infraestructures, serveis i medi ambient)
13	Dr. Josep Maria Tormos	Director de recerca

14	Sra. Àngels Hervàs	Cap de treball social
15	Sra. Laura Pla	Coordinadora de voluntariat

Relació de la documentació lliurada a l'auditor:

- Menú documentació auditoria 2022
- Informe Auditoria Llei Oficial de Protecció de Dades LOPD 2020.
- Informe audit protecció dades I. GUTTMANN (evidència de comunicació a direcció).
- Registre Activitats del Tractament IG 2022.
- Sol·licitud Inscripció DPD Maig 2018.
- Formulari de nomenament de DPD Institut Guttmann maig 2018.
- Exp1519339806915priv AEPD (codis d'inscripció dels fitxers a l'AEPD).
- Manual d'Acollida Guttmann - Versió maig 2022.
- Document d'informació i compromís del professional.
- Manual Usuari Portal badalona V3.
- Model Consentiment Revisió Mèdica 2020 ca.
- Full dades personals CAT-CAST.
- Enquesta Acollida (Hig.Mans + RCP).
- Full de Documentació Rebuda (Hig.Mans + RCP) Bdn.
- Guia Higiene de Mans i Reanimació.
- Incidències de 2020 a 2022 (mostra en diferents documents).
- Formació Pla d'Autoprotecció 2022 BADALONA.
- Formació LOPD 2021_BDN
- Annex 08 Compromís Professionals Ca_LOPD.
- Anexo 09 Autorización Paciente para el tratamiento de datos 2020 IG cast.
- Informació per al tractament de dades de caràcter personal (pacients).
- Annex 17 Sistema de seguretat i pla de contingències.
- Annex 21 Esquema de la xarxa.
- Autorització gravació sessions formatives 2019 ca.
- Autorització presa d'imatges i veu 2021 ca.
- Autorización Toma imagenes y voz 2021 es.
- Autorització presa d'imatges i veu per part del representant legal 2021 ca.
- Autorización toma de imagenes y voz por parte del representante legal 2021 es
- Autorització Titol_Centres Estudi.
- Declaració CODI ÈTIC CAT-CAST
- Contracte de compromís de voluntariat.

- Models per a l'exercici dels drets de les persones: formularis de dret d'accés, rectificació, supressió, oposició, limitació i portabilitat.
- Exercici de drets (mostra de casos reals).
- Mostra de contractes d'encàrrec de tractament i compromís de confidencialitat: Doctodata, S.L. (proveïdor de software i expedient digital), Gracare, S.A. (subministrament d'ajudes tècniques als pacients), Suministros Ortopédicos Meridiana, S.L. (ajudes tècniques als pacients), Qvitec Centre d'Ajudes Tècniques, S.L. (ajudes tècniques als pacients), Extreme Information Technologies (serveis de suport i manteniment de la intranet).
- Contracte marc d'accés a la informació vinculat al contracte de servei de tractament de lesions neurològiques amb Mútua de Navarra.
- Registre d'accessos (mostra).
- Registre d'accessos GNPT (mostra).
- Informe abril datos (comunicació sobre revisió d'accessos indeguts).
- Informe marzo datos (comunicació sobre revisió d'accessos indeguts).
- Document de Seguretat Fitxer Administració 2019.
- Document de Seguretat fitxer BBHI 2019.
- Document de Seguretat Fitxer Externs 2019.
- Document de Seguretat Fitxer Investigació 2019.
- Document de Seguretat Fitxer Pacients 2019.
- Document de Seguretat Fitxer Personal 2019.
- Document de Seguretat Fitxer Prevenció del blanqueig de Capitals 2019.
- Document de Seguretat Fitxer Reclamacions 2019.
- Document de Seguretat Fitxer Videovigilància 2019.
- General Avaluació Riscos 24-03-2020 V3.
- AL-1-RS-PDP-026001-ca Avaluació de Riscos 2022 v4.
- PC-3-SI-LPD-0009-ca-Document de Seguretat fitxer GNPT 2019.
- Auxiliar Infermeria UH Avaluació de Riscos 2020_v5.
- Informe Avaluació Impacte Tractament Pacients.
- Informe Avaluació Impacte Tractament Personal.
- Informe Avaluació Impacte Tractament ECOFIN.
- Informe Avaluació Impacte Tractament Reclamacions.
- Informe Avaluació Impacte Tractament RRPP Amics.
- Informe Avaluació Impacte Tractament Vídeos Formació.
- Informe Avaluació Impacte Tractament GBL.
- Informe Avaluació Impacte Tractament Voluntaris.
- Informe Avaluació Impacte Tractament TBC.
- Informe Avaluació Impacte Tractament Videovigilància.

- Informe Avaluació Impacte Tractament GNPT.
- Informe Avaluació Impacte Tractament Blanqueig de Capitals.
- Informe Avaluació Impacte Tractament Empremtes dactilars.
- Informe Avaluació Impacte Tractament Medxat.
- Informe Avaluació Impacte Tractament AQuAS.
- Informe Final Avaluació Impacte Tractament AQuAS.
- Informe Avaluació Impacte Tractament TBC.
- Informe Avaluació Impacte Tractament HCE.
- AL-1-RS-PDP-026001-ca Avaluació de Riscos 2022 v4

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, l'entitat 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.

Segons les informacions i evidències proporcionades, l'entitat ja té implementada una política de realització biennal d'auditories sobre protecció de dades. Tal com podem comprovar amb l'evidència aportada, el darrer informe d'auditoria porta data de 23/06/2020. D'altra banda, els resultats de l'auditoria es van a elevar a la direcció de l'entitat. També consta que es van adoptar accions concretes com a conseqüència d'aquest resultat. El document "*Informe audit protecció dades I. GUTTMANN*", que s'ha aportat com a evidència, documenta que l'informe i el seu resultat es van comunicar a la direcció de l'entitat.

Per tot plegat, podem constatar que ja s'està aplicant correctament una mesura de seguretat de realització d'auditories biennals, el resultat de les quals s'eleva a la direcció de l'entitat. Com a possible millora, però, caldria documentar les previsions de millora que s'adoptin com a conseqüència del resultat.

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.

En el cas de l'entitat, els tractaments que du a terme, pel volum i la sensibilitat de les dades tractades, poden implicar un risc per als drets i les llibertats. D'altra banda, també s'hi tracten dades de categoria especial, com ho són per exemple les dades de salut dels pacients. Per tant, 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, l'entitat manifesta i pot evidenciar que ha elaborat un RAT a través del document "*Registre Activitats del Tractament IG 2022*", que aporta per a la seva revisió i que, tal com es pot comprovar, identifica diferents activitats de tractament amb els següents noms:

- Pacients
- Personal
- Administració
- Reclamacions
- Externs RRPP
- Externs Amics
- Videos Formació
- Externs GBL
- Externs S&L GC
- Externs Docència
- Externs Voluntaris
- Externs TBC
- Vídeo Vigilància
- Investigació
- GNPT
- BBHI
- Blanqueig
- Empremtes Digitals
- Medxat
- AQUAS
- Nova Hce
- Parking
- Cafetería y cocina
- Estudiantes master, Residentes y Prácticas

Es comprova que el RAT realitzat per l'entitat, un document Excel, ja conté correctament tots els camps previstos per l'article 30 (finalitats del tractament, categories de dades, tipus d'interessats, destinataris de les dades i períodes o criteris de conservació, entre d'altres), a més d'altres informacions addicionals que contribueixen a la definició i comprensió dels tractaments, com ara si s'han fet anàlisis de risc o avaluacions d'impacte. En efecte, com a novetat important del RAT aportat com a evidència és que ara identifica, respecte a cada activitat de tractament, si se n'ha fet una anàlisi de riscos o una avaluació d'impacte.

Es comprova que al RAT ja hi ha un camp sobre transferències internacionals de dades, però que en totes les activitats de tractament s'indica que no n'hi ha. En tot cas, en el supòsit que es constati l'existència de transferències internacionals de dades en un futur, caldrà tenir en compte que hauran de fer-se constar al RAT i fonamentar-se en una causa de legitimació prevista al RGPD. En aquest sentit, el règim legal conegut com a Privacy Shield, que fins fa poc permetia legitimar transferències internacionals de dades a Estats Units, ja no és vàlid, segons han determinat autoritats judicials europees.

El camp de terminis o criteris de supressió indica que, en la majoria de casos, es preveu un termini "indefinit" de conservació. Tenint en compte que la conservació de les dades ha de venir limitada per la desaparició de la necessitat que en va justificar la recollida, caldria revisar si es pot concretar un termini o criteri de forma més precisa en cada cas.

Cal tenir en compte que l'activitat principal desenvolupada per l'entitat, la que implica un tractament més massiu i sensible de dades i que constitueix la base del seu objecte fundacional, és la corresponent a la prestació d'assistència sòcio-sanitària, especialitzada en aquest cas al tractament de lesions medul·lars, danys cerebrals i discapacitats d'origen neurològic.

Val a dir que, a banda de les qüestions comentades, el RAT també s'ha actualitzat d'ençà de la darrera auditoria amb noves activitats de tractament, que són: *Medxat*, *AQUAS*, *Nova Hce*, *Parking*, *Cafetería y cocina*, *Estudiantes máster*, *Residentes y Prácticas*. Aquestes activitats corresponen a nous canals, serveis o aspectes que s'han volgut identificar de forma particular en aquest registre.

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

●	Com a possible aspectes a millorar del RAT, caldria revisar correctament en cada activitat de tractament la possible existència de transferències internacionals de dades i els terminis o criteris de supressió de les dades.

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, que ha de regir tot tractament de dades.

L'entitat disposa de diferents documents de seguretat, que descriuen correctament, de manera integral, la política de protecció de dades i les mesures de seguretat que aplica l'entitat. Aquestes mesures, tal com podem corroborar, es corresponen en bona part amb les que ja preveia l'antic Reglament de 2007 (RLOPD) que desenvolupava la LOPD anterior. Tot i que estem parlant d'una normativa que ja no és la referent, les mesures de seguretat que hi apareixien definides continuen essent un referent rellevant.

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. D'aquesta manera, l'entitat continua aplicant les mesures de seguretat citades, previstes al RLOPD, 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.

D'altra banda, l'AEPD ha definit unes mesures de seguretat mínimes obligatòries que han de complir tots aquells tractaments de dades que suposin un risc escàs. Aquestes mesures de seguretat, de tipus organitzatiu i tècnic, cal garantir-les en tot cas i sobre tots els tractaments. Tal com podem comprovar a través de la documentació aportada a aquesta auditoria, l'entitat assumeix de forma implícita totes aquestes mesures.

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 espais 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'ença 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 ✓ 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. ✓ 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 avaluat en diferents punts d'aquest informe.

Els tractaments que realitza l'entitat 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.

Podem observar una descripció detallada de com es tracten les dades en les diferents activitats de tractament i de les mesures de seguretat que s'hi apliquen en diferents documents desenvolupats per l'entitat, com ara:

- Documents de seguretat i annexos.
- RAT de l'entitat.
- Annex 17 Sistema de seguretat i pla de contingències.

És en aquest Annex 17 on podem observar de forma exhaustiva les mesures de seguretat que ha definit i aplica l'entitat actualment. Comprovem que tots els documents estan actualitzats.

El document "*Annex 21 Esquema de la xarxa*" presenta un esquema general de la xarxa informàtica de l'entitat i de mesures de seguretat previstes a nivell general.

Comprovem, per la documentació aportada com a evidència, que l'entitat ha dut a terme un esforç important d'anàlisi de risc en relació a cadascuna de les diferents activitats de tractament, determinant en cada cas la necessitat de fer una avaluació d'impacte i realitzant la corresponent avaluació, en cas necessari. A aquest efecte, s'han fet servir models d'Excel, que són evidència de la gestió proactiva de l'entitat a l'hora de conèixer, analitzar i minimitzar riscos. Tots els informes d'avaluació d'impacte s'han fet en format Excel durant els darrers dos anys i constitueixen una novetat important d'ençà de la darrera auditoria. Comprovem que ja segueixen un format que permet presentar una descripció sistematitzada del tractament, analitzar-ne la necessitat i proporcionalitat, identificar-ne els riscos quantificats des del punt de vista de la probabilitat i

l'impacte, associats a unes mesures de seguretat destinats a minimitzar-los i a un risc residual quantificat. Com a possible millora, caldria distingir entre el risc inherent dels riscos (ara no s'hi identifica) i el risc residual, que és el que quedaria com a conseqüència d'aplicar les mesures de seguretat proposades. No obstant, de forma general, els informes compleixen la funció de permetre identificar i minimitzar els riscos associats a una determinada activitat de tractament.

D'acord amb una recent sentència de 15 de febrer de 2022, el Tribunal Suprem ha confirmat que l'aplicació de mesures de protecció de dades no és una obligació de resultat, sinó de mitjans. Això lliga amb el principis de responsabilitat proactiva i d'*accountability* que han d'influir en l'actuació de qualsevol entitat i en la necessitat de documentar i demostrar l'adopció de mitjans i mesures de seguretat adequades en la protecció de dades.

Per tot plegat, amb les informacions i evidències documentals aportades, podem concloure que l'entitat ja du a terme una gestió proactiva del risc i té previst un procediment per a l'anàlisi i realització d'avaluacions d'impacte, que seria aplicable en determinades situacions d'imprevisibilitat relativa a l'impacte.

Àrees de millora

●	Els documents aportats a aquesta auditoria com a evidències, sobretot l'"*Annex 17 Sistema de seguretat i pla de contingències*" demostren que s'han tingut en compte els riscos que impliquen les activitats de tractament de dades i que s'han implementat mesures de seguretat en relació a aquests riscos. Aquestes mesures, tal com estan definides i plantejades, responen en bona mesura a les que ja preveia l'antic RLOPD i resulten adequades; en tot cas, caldrà que sempre es puguin revisar i actualitzar, tenint en compte les necessitats de nous tractaments que puguin sorgir i dels principis de privacitat per disseny i per defecte. Constatem especialment l'evidència documental de la realització d'anàlisis de riscos i avaluacions d'impacte en relació a les activitats tractament. Les avaluacions d'impacte s'han dut a terme en equip amb la participació del DPD, i en aquest punt cal recordar que no seria correcte que fos el DPD qui elaborés directament els informes d'avaluació d'impacte, ja que això plantejaria problemes de compatibilitat amb les seves altres funcions d'assessorament i supervisió. Els informes d'avaluació d'impacte revisats, en termes generals, són correctes i s'ajusten a les característiques previstes que han de tenir aquests informes. Com a possible millora, caldria que incloguessin la diferència entre el risc inherent (previ a l'aplicació de mesures de seguretat) i el risc residual (el que quedaria després d'aplicar les mesures de seguretat), identificat i quantificat en cada cas tant pel que fa a l'impacte com a la probabilitat. També seria necessari incloure als informes les mesures proposades per a la minimització del risc i, posteriorment, disposar d'evidències del seguiment que es fa sobre l'aplicació dels informes. Les autoritats de control han publicat guies sobre criteris i metodologia a emprar en l'elaboració d'avaluacions d'impacte, tant l'Autoritat Catalana de Protecció de Dades (APDCAT) com l'Agència Espanyola de Protecció de Dades (AEPD). L'AEPD ha publicat una eina online sobre la matèria que s'anomena GESTIONA.

5.4. DELEGAT DE PROTECCIÓ DE DADES

Base legal: Article 37 RGPD

D'acord amb les informacions i evidències aportades, l'entitat ja va procedir a nomenar internament el Sr. Javier Remacha Fuentes com a delegat de protecció de dades (DPD). Aquest nomenament es va comunicar a l'APDCAT el dia 01/05/2018. L'autoritat de control va comunicar la recepció de la comunicació en data 11/05/2020, assignant-li el codi 0199/698/2018. S'aporten i es comproven la comunicació i la resposta de l'autoritat de control.

La figura del DPD consta a tots els documents de seguretat, juntament amb una descripció exhaustiva de les seves funcions. També consta a l'organigrama de l'entitat. En general, per tant, s'ha fet difusió suficient de la figura del DPD. Tal com es pot comprovar, 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 forma de comunicar-s'hi. També apareix en la informació legal que es proporciona a tot el personal a través del manual d'acollida. Aquesta informació es proporciona a totes les noves incorporacions al personal i és consultable a través de la intranet corporativa.

El DPD té altres responsabilitats a l'entitat. En particular, és responsable de l'Oficina Tècnica de Direcció. Entre d'altres, desenvolupa tasques de protecció de dades, prevenció de riscos laborals i responsabilitat social corporativa. 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. D'altra banda, el DPD té coneixements jurídics i demostrada formació i experiència en matèria de protecció de dades. En particular, consta que ha assistit a la formació específica impartida per la Unió Catalana d'Hospitals en aplicació del seu Codi Tipus.

D'acord amb les evidències proporcionades, els documents de seguretat ja es defineixen les accions i tasques que s'atribueixen al DPD i que constitueixen una definició sobre la seva actuació; d'altra banda, el DPD du a terme diferents accions d'informació a la gerència de l'entitat, que podem comprovar, com són:

- Cada mes, envia la verificació dels accessos.
- Mensualment, envia verificació dels accessos del GNPT.
- Mensualment, envia llistat d'incidències (informàtiques i de seguretat).
- Cada dos anys, envia el resultat de l'auditoria.
- Setmanalment (de forma aproximada), informa sobre aspectes de la seva àrea.

També es preveuen plans de formació sobre protecció de dades coordinats pel DPD. En particular, es té en compte el document "*5 Formació LOPD 2021_BDN*", que és una presentació sobre protecció de dades que es proporciona al personal.

Val a dir, finalment, que, com a conseqüència de la crisi causada per la pandèmia de Covid-19, es constata un acord sobre teletreball i protecció de dades que ha estat elaborat i s'ha fet signar a tot el personal.

No detectada

▲	

5.5. ENCARREGATS DEL TRACTAMENT I PROVEÏDORS SENSE ACCÉS A DADES

ENCARREGATS DEL TRACTAMENT

Base legal: Article 28 RGPD i disposició transitòria cinquena LOPDGDD

Els documents de seguretat de l'entitat ja contenen instruccions i previsions sobre com l'entitat ha de procedir correctament en la seva relació amb encarregats del tractament de les dades, d'acord amb la normativa vigent. En concret, s'hi estableix la necessitat de tenir contractes signats amb els encarregats del tractament i fer-los acceptar les mesures de seguretat definides pel responsable. A aquest efecte, s'hi preveu que als contractes mercantils s'hi afegeixi una clàusula, i que en alguns casos, s'incorpori una ampliació de contracte a contractes ja signats.

El document Excel "*Llistat actualitzat maig'22*" aportat a aquesta auditoria conté una relació exhaustiva i actualitzada de proveïdors de servei. Mitjançant aquest document, el DPD pot controlar aspectes relatius a aquests proveïdors: si són o no encarregats, la data del contracte, la seva vigència i si tenen o no la consideració d'encarregat. Comprovem també que l'entitat disposa d'un model de contracte d'encàrrec de tractament de dades degudament actualitzat i ajustat al RGPD.

No consta que hi hagi implementat un protocol específic sobre selecció de proveïdors, per tal de poder garantir per part del responsable del tractament que es contracta amb qui reuneix els requisits i s'ajusta als requeriments de la normativa.

En la darrera auditoria es va detectar que determinats docents a l'àrea de docència havien de signar un contracte d'encàrrec de tractament, però no consta que aquests contractes s'hagin signat en el "*Llistat actualitzat maig'22*".

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

ET DETECTATS	SERVEI PRESTAT	CON-TRAC-TE	COMENTARIS
Doctodata, S.L.	Serveis de software i expedient digital.	✓	El contracte és correcte i ajustat a la normativa vigent
Gracare, S.A. (subministrament d'ajudes tècniques als pacients)	Ajudes tècniques als pacients	✓	El contracte és ajustat a la normativa vigent aplicable.
Suministros Ortopédicos Meridiana, S.L.	Ajudes tècniques als pacients	✓	El contracte és ajustat a la normativa vigent aplicable.
Qvitec Centre d'Ajudes Tècniques,	Ajudes tècniques als pacients	✓	El contracte és ajustat a la normativa vigent aplicable.

S.L.			
Extreme Information Technologies, S.L.	Serveis de suport i manteniment de la intranet	✓	El contracte és ajustat a la normativa vigent aplicable.
Professors de l'àrea de docència.	Serveis de docència	×	Els professors de l'àrea de docència són encarregats del tractament de les dades dels alumnes.

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. Per tant, un cop expirat aquest termini, cal tenir en compte que ja no hi poden haver contractes signats sota el règim legal anterior.

A partir del 25 de maig de 2022 tots els nous contractes amb Encarregats de Tractament han de respectar el contingut que preveu l'article 28 del RGPD.

L'entitat actua com a encarregada del tractament de la Mútua de Navarra, d'acord amb el document "*contracte marc d'accés a la informació vinculat al contracte de servei de tractament de lesions neurològiques*". Aquest contracte d'encàrrec de tractament és ajustat a la normativa i genèric, perquè no concreta l'abast dels serveis que impliquen el tractament de dades, sinó que deixa aquesta concreció en un contracte de servei. Val a dir que, encara que es pugui entendre que hi pot haver un tractament de dades en la prestació de serveis a pacients, la prestació assistencial no es pot realitzar en condicions d'encàrrec, sinó de responsable del tractament.

Àrees de millora

●	Com a elements de millora en aquest apartat cal considerar els següents aspectes: • Revisar que no hi hagi contractes d'encàrrec de tractament que encara estiguin signats sota el règim legal anterior i, si és el cas, actualitzar-los. • Adoptar un protocol que estableixi les bases per a la selecció i tractament amb encarregats del tractament, tenint en compte criteris i principis de protecció de dades. • Revisar la situació dels docents externs adscrits a l'àrea de docència, comprovar si tenen accés a les dades i, si és el cas, fer-los signar un contracte d'encàrrec de tractament de dades.

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 24 RGPD

Situació actual

L'entitat és conscient que determinats serveis prestats per altres persones o entitats impliquen no haver de tenir cap accés a dades personals, però podrien suposar un accés involuntari o accidental a les dades. Per a prevenir aquesta situació de risc i un possible accés indegut, correspon aplicar un compromís de confidencialitat.

Amb el document Excel "*Llistat actualitzat maig'22*" comprovem que es manté una relació actualitzada de proveïdors que tenen accés a dades, qualificats com a encarregats de tractament de dades, que es diferencien dels que no tenen accés a dades. En funció del tipus de proveïdor i de si té o no accés a dades, se li fa signar un model de contracte d'encàrrec de tractament o se li fa signar un compromís de confidencialitat que reflecteixi la realitat de la situació i preservi la confidencialitat i la seguretat de les dades, de conformitat amb el RGPD.

Comprovem que efectivament tots els proveïdors sense accés a dades ja s'identifiquen al document i que ja hi ha també un procediment previst per a fer-los signar un model de compromís de confidencialitat. L'entitat disposa d'un model d'acord de confidencialitat adequat a la normativa vigent. S'aporta com a evidència a aquesta auditoria una mostra de compromís de confidencialitat signat.

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS SIGNAT	COMENTARIS
José Miguel Molina Llop	Serveis de traducció	▲	
Manel Cardiel Tarragó, auditor de SGS International Certification Services Iberica, S.A.	Servei d'auditoria i certificació	▲	

No detectada

▲	

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

En punt anterior en què es feia referència específica al RAT ja hem indicat les activitats de tractament previstes per l'entitat. Analitzem ara de manera general la legitimitat de les diferents activitats de tractament de dades que du a terme l'entitat i que es fan constar al RAT, que són les següents:

- **Pacients**

Aquest tractament de dades és conseqüència dels serveis d'assistència sanitària que presta l'entitat. De la prestació assistencial de tipus sanitari o social deriva que l'entitat hagi de recollir i tractar dades de categoria especial, especialment de salut. No obstant, aquest tractament, com que es fonamenta en la prestació de serveis d'assistència sanitària i social, és legítim, de conformitat amb l'article 9.2 lletra h) del RGPD.

La prestació assistencial es pot classificar en dues grans àrees diferenciades: la pública, que correspon al servei públic concertat amb CatSalut, fonamentada en l'existència d'una regulació legal, d'acord amb la base legal de l'article 6.1.c) del RGPD, i la que deriva d'una concertació amb les mútues o amb el pacient estranger, que es basaria en l'existència d'una relació contractual, d'acord amb l'art. 6.1.b) del RGPD. En general, els tractaments ja s'ajusten a criteris de proporcionalitat i adequació a la finalitat del tractament i a les necessitats de la prestació del servei.

De forma ordinària, al pacient que encara no té una fitxa oberta se li extreuen les dades del Registre central d'assegurats del CatSalut (RCA). Si no té història (per exemple, els pacients estrangers), se li obre una fitxa i se li recullen dades com ara el nom i cognoms, data de naixement, domicili, targeta sanitària, telèfon de l'acompanyant i mitjans de contacte. D'acord amb el document de seguretat corresponent, a cada pacient (o representant legal) se li lliura el document "*Informació per al tractament de dades de caràcter personal*", que s'arxivarà a la història clínica degudament signat. Aquest document conté ja de forma completa tota la informació sobre el tractament de les dades i un seguit d'autoritzacions expresses, que el pacient pot acceptar o no lliurement. El responsable del tractament determina que aquesta tasca correspon al servei d'admissions.

Els usos que l'entitat pretén realitzar de les dades amb el consentiment del pacient són pertinents i proporcionats, ja que responen a interessos del servei, de l'entitat i del propi pacient. En concret, es demana autorització per a informar sobre el número de l'habitació a les visites, per a emetre recordatoris de visita per mitjans electrònics, per a rebre informació sobre novetats de l'entitat, per a participar en enquestes de satisfacció i per a tractar les dades de salut amb finalitats de recerca i difondre-les de forma pseudonimitzada, en cas necessari. Tots aquests usos són legítims, i la forma legítima de poder-los fer és a través del consentiment exprés del pacient, tal com ha previst correctament l'entitat.

En determinats casos, l'entitat pot recollir i fer servir la imatge de pacients, basant-se en l'obtenció del consentiment exprés, tal com s'estableix a l'article 6.1.a RGPD. Des de

l'àrea de comunicació, en aquests casos, es faria signar un model de consentiment. Constatem l'existència de diferents models de consentiments utilitzats en aquesta àrea per a aquesta finalitat.

D'altra banda, en relació al tractament de dades assistencials, cal tenir present que l'adopció de noves tecnologies de comunicació en la prestació dels serveis pot implicar la necessitat de realitzar una avaluació d'impacte.

- **Personal**

Pel que fa a la selecció i contractació del personal i la seva formació, la finalitat de l'activitat de tractament és la gestió de la relació laboral i l'organització dels recursos humans a l'entitat. La base jurídica que la permet es fonamenta en la preparació i execució d'un contracte de treball, de conformitat amb l'article 6.1.b) RGPD.

En el cas de la prevenció de riscos i vigilància de la salut, la legitimitat del tractament també deriva del compliment d'una obligació legal, d'acord amb l'article 6.1.c) RGPD. L'elaboració de les nòmines i la gestió de recursos humans en general es du a terme internament per part de l'entitat.

L'entitat du a terme els seus propis processos de selecció de personal i fa servir a aquest efecte un formulari de la seva web, a l'apartat "Treballa amb nosaltres, on publica les ofertes de treball, que la mateixa entitat s'encarrega també de difondre a través d'altres canals com LinkedIn. En general, els candidats poden emplenar el formulari i adjuntar el seu CV a través d'aquesta eina i, durant aquest procés, han de marcar necessàriament dos quadres de *checkbox*, a través dels quals presten el consentiment i accepten un "avís legal" i una "Política de privacitat". Comprovem que l'enllaç de la "Política de privacitat" condueix a una informació legal que és idèntica que la de l'"avís legal", probablement per error. En aquest sentit, l'única informació legal que es proporciona sobre protecció de dades és la que es troba al mateix formulari, però és incompleta i no s'ajusta a l'art. 13 RGPD. En principi, les dades es conservarien a la plataforma de la web durant 12 mesos, després dels quals tornarien a demanar el consentiment.

Quan hi ha una decisió d'incorporar un candidat a l'organització, per part de recursos humans es fa una comunicació a l'àrea d'informàtica a través d'una app. En aquesta comunicació es defineix el perfil d'accés de la nova incorporació, segons autorització del responsable de la seva àrea.

Quan la persona entra a treballar a l'entitat per primer cop, se li aplica un procés d'acollida que implica proporcionar i fer signar, si és el cas, els següents documents, que poden ser rellevants en relació a protecció de dades:

- Informació sobre protecció de dades, que és conforme a art. 13 RGPD.
- Compromís de confidencialitat
- Manual de bones pràctiques.
- Acord sobre teletreball.

Tots els documents citats han estat aportats per l'entitat a aquesta auditoria i, després de revisar-los, comprovem que estan actualitzats i que ja permeten proporcionar una informació exhaustiva i completa sobre el tractament de les dades personals, de

conformitat amb l'art. 13 RGPD. No consta que es recullin més dades del personal de les que siguin necessàries per a l'elaboració del contracte i la gestió de la relació laboral.

Durant el procés d'acollida es proporciona al nou membre del personal una targeta d'identificació. D'entrada, la imatge del treballador només es fa servir per a la targeta d'identificació i per a la intranet, segons l'interès legítim de l'entitat. Si es volguessin fer altres usos de la imatge, es recolliria el consentiment del treballador i la base jurídica prevista seria la prestació del consentiment de l'interessat. Comprovem que els models documentals de recollida del consentiment ja proporcionen una informació correcta sobre el tractament de la dada de la imatge del personal, d'acord amb l'art. 13 del RGPD, i permet a la persona interessada prestar el seu consentiment en els termes previstos pel RGPD. A la pràctica, tanmateix, tal com comentàvem, la imatge del treballador només es fa servir generalment per a la presentació de la persona dins el sistema d'intranet i en la targeta d'identificació.

En general, el personal laboral gestiona les seves pròpies dades i alguns elements de la relació laboral des del Portal INTEGHRO. A través d'aquesta aplicació, el treballador pot accedir a les seves nòmines i dades fiscals. D'altra banda, fan servir el portal BOLD per a gestionar les seves vacances, permisos, canvis de torn.

Segons les informacions proporcionades, ja hi ha implementat un sistema de fitxatge i de registre de jornada, que es fa a través de marcar l'empremta digital. En el seu moment, ja es va fer un informe d'avaluació d'impacte sobre aquest tractament, de què s'aporta evidència.

La prevenció de riscos laborals es du a terme internament per part de l'entitat, mentre que la vigilància de la salut la realitza una empresa externa, ASPY. Les cobertures relatives a accidents laborals corresponent a la Mútua Universal.

Respecte a la implementació del teletreball com a conseqüència de la recent emergència sanitària causada per la Covid-19, s'ha desenvolupat un acord específic sobre teletreball, que s'ha comunicat i s'ha fet signar al personal. Per tant, ja consta que l'entitat ha definit unes previsions per escrit sobre el teletreball, determinant quines garanties i mesures implica des del punt de vista de la seguretat i la privacitat, i n'ha informat el personal de manera adequada.

No consta que l'entitat faci un ús del telèfon o 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. No consten usos o tractament de les dades dels treballadors que puguin tenir la condició de desproporcionats o innecessaris des del punt de vista de la gestió de la relació laboral. No consta, per exemple, que es facin tractaments de geolocalització o de videovigilància amb finalitats de control laboral.

- **<u>Administració</u>**

Aquest tractament té per finalitat la gestió comptable i la facturació corresponents a l'activitat de prestació assistencial i social duta a terme per l'entitat. La base jurídica del

tractament és la necessitat de gestionar contractualment i facturar els serveis prestats per l'entitat, de conformitat amb l'article 6.1.b) RGPD.

En el cas de pacients particulars, el tractament de les seves dades es du a terme a través del SAP La informació sobre el tractament ja s'ha proporcionat en el moment que s'incorporen les seves dades. Si són pacients de CatSalut o de mútues, ni tals sols es disposa de les seves dades per a la gestió de la facturació.

La gestió de proveïdors pot implicar un tractament de dades personals, encara que, en molts casos, quan els proveïdors són persones jurídiques, les dades personals tractades siguin residuals o insignificants. En d'altres casos, podrien haver-hi dades de proveïdors que fossin persones físiques, i llavors les dades recollides serien les necessàries per a la facturació i la gestió comptable.

D'acord amb les informacions proporcionades, són molt poques les dades personals que poden haver-hi en aquest tractament i, en tot cas, són dades de contacte, sobretot. En qualsevol cas, si en algun moment es valora l'existència d'un tractament de dades de proveïdors clarament identificable, caldrà implementar procediments d'informació de conformitat amb l'art. 13 de la RGPD.

- **Reclamacions**

La finalitat d'aquest tractament és poder facilitar i gestionar un un procediment de reclamacions i/o suggeriments, de conformitat amb la Llei 15/1990, d'ordenació sanitària de Catalunya, i amb la Instrucció 03/2004. Per tant, la base legítima del tractament és el compliment d'una obligació legal.

Aquest procediment el pot iniciar l'usuari dels serveis emplenant un formulari. En aquests formularis ja s'inclou una nota a peu de pàgina que informa adequadament sobre el tractament de les dades, tal com preveu l'art. 13 RGPD.

És el personal de l'àrea d'atenció a l'usuari que s'encarrega de proporcionar aquests formularis i fer-ne seguiment.

- **Externs**

L'entitat disposa en un únic document de seguretat d'una previsió de tractament de dades relatives a col·lectius de persones físiques amb qui manté algun tipus de vinculació comercial o de prestació de serveis diferent de les previstes en d'altres tractaments. Són els tractaments identificats al "*Document de Seguretat Fitxer Externs 2019*", al qual podem afegir també en aquest apartat el tractament de vídeos necessaris en processos de gravació, ja que preveu la captació de la dada de la imatge i la veu de persones vinculades a la formació (alumnes i professors, que tenen la condició de col·laboradors externs). En resum, per tant, els considerats "Externs" són els següents col·lectius i aspectes del tractament:

- Voluntaris
- Treballadors en benefici de la Comunitat
- Amics de l'Institut Guttmann
- Empreses i col·laboradors externs

- Alumnes
- Videos formació

Aquests col·lectius coincideixen amb les activitats de tractament identificades al RAT com a "Externs Voluntaris", "Externs TBC", "Externs Amics", "Externs docència" i "Video formació". La base jurídica del tractament és generalment, en tots aquests casos, l'existència d'una vinculació contractual, de conformitat amb l'article 6.1.b) RGPD, i la finalitat del tractament seria la gestió dels serveis corresponents, tant si aquests col·lectius actuen com a receptors o prestadors. En el cas dels vídeos, però, la base jurídica és el consentiment de la persona interessada, que ha de signar un document de consentiment exprés.

En el cas dels voluntaris, es poden donar d'alta a través d'un formulari de la web, però comprovem que, en aquest cas, hi ha una informació molt bàsica sobre el tractament de les dades (incompleta, des del punt de vista de l'art. 13 RGPD) i la possibilitat d'acceptar un avís legal, que conté una informació legal sobre diferents aspectes, però que no completa la informació bàsica sobre protecció de dades. Per tant, no es compleix a través de la web l'obligació de proporcionar informació sobre el tractament en aquest cas.

Tal com es pot comprovar amb la documentació aportada relativa a la gestió concreta de cada col·lectiu i dels serveis corresponents, es comprova específicament que en cada cas hi ha un contracte o matrícula específica (també en el cas dels voluntaris), un procediment d'acollida, unes instruccions sobre seguretat, una informació sobre protecció de dades (inclosa al contracte) i un compromís de confidencialitat que la persona ha de signar. En el cas dels col·laboradors externs, que inclouen els professors, es recullen les seves dades mitjançant un formulari que ja inclou la informació de l'art. 13 RGPD.

La gestió dels treballadors en benefici de la comunitat i el tractament de les seves dades es fonamenta en la col·laboració que l'entitat manté amb el Departament de Justícia, de qui depenen les dades en darrera instància.

Pel que fa als "*Amics de l'Institut Guttmann*", són persones que lliurement decideixen fer donacions puntuals o periòdiques a l'entitat i, a canvi, reben alguna prestació. Aquestes persones poden inscriure's a través de la web de l'entitat, on hi ha un formulari de recollida de dades i un avís legal. Es comprova que la informació que proporciona aquest avís legal de la web s'ajusta a l'antiga legislació; per tant, no és correcte i caldria actualitzar-la. D'altra banda, es constata que en alguns casos també es poden inscriure persones en aquest grup sense passar per la web, de manera que es recollirien les seves dades sense que hi hagi un procés de proporcionar-los una informació sobre el tractament, de conformitat amb l'article 13 RGPD. Per tant, cal que es determini la necessitat de poder unir-se a aquet col·lectiu a través d'un procediment que permeti sempre proporcionar una informació sobre el tractament, com ja passa a través d'emplenar el formulari de la web.

No es detecten tractaments que puguin tenir la condició de desproporcionats o innecessaris des del punt de vista de la gestió dels serveis i de la finalitat del tractament.

- **Externs RRPP:**

El RAT identifica un tractament dit "Externs", que no apareix desenvolupat al document de seguretat titulat "Externs". Es tracta de dades personals, que es tracten amb la finalitat de facilitar la comunicació de l'entitat. La base jurídica és el consentiment de la persona interessada.

La revista "*Sobre Ruedas*", que té una periodicitat quadrimestral , s'envia als pacients que ho han autoritzat expressament i per escrit durant la seva primera visita.

La revista "*Fulls*", que té una freqüències semestral, s'envia als treballadors de l'entitat per defecte, ja que s'entén aquí que pot aplicar-s'hi una base jurídica d'interès legítim. Els treballadors podrien exercir en qualsevol moment el seu dret d'oposició, de manera que deixarien llavors de rebre la revista. També a com comunicació als treballadors s'envia la newsletter "*Guttmann al dia*" amb una freqüència quinzenal.

Les xarxes que es fan servir per a la comunicació són Facebook, Twitter, Instagram, LinkedIn i YouTube. Cal tenir en compte que, d'acord amb el posicionament actual de les autoritats europees, l'ús de certes xarxes socials (com passa ara amb Facebook) implica l'existència de transferències internacionals de dades a països no segurs. Per tant, és important que l'ús d'aquestes xarxes i les transferències que suposen estigui degudament informat a les persones interessades i que se'n reculli, si és el cas, el consentiment exprés per a la transferència.

En alguns casos es pot crear una web específica per a la gestió d'un esdeveniment mitjançant una empresa subcontractada. Els participants poden inscriure's a través d'un formulari de la web, on ja consta un avís legal amb informació de l'art. 13 RGPD. En aquest cas, el formulari també preveu que es presti el consentiment per al tractament de les dades.

Pel que fa les imatges del personal, només es publiquen o difonen quan s'hi ha consentit expressament per escrit. Comprovem que el personal ja signa un model d'autorització de consentiment per a l'ús de la imatge amb finalitats de comunicació, que és correcte.

- **Externs GBL i Externs S&L GC:**

Aquestes dues activitats de tractament corresponen a dades obtingudes i tractades en la prestació dels serveis Guttmann Barcelona Life i Sport&Life Guttmann Club. Aquests dos tractaments no estan desenvolupats al document de seguretat corresponent als Externs, ni se n'ha analitzat informació o documentació específica en aquesta auditoria. No obstant, consisteixen en una extensió de la prestació assistencial sòcio-sanitària que realitza l'entitat. La base jurídica seria, per tant, la prestació sòcio-sanitària, juntament amb el compliment del contracte que va vinculat a la prestació d'aquests serveis.

En el cas de Guttmann Barcelona Life, consisteix en un equipament social format per apartaments domotitzats i adaptats. A través d'un procediment de selecció, persones amb discapacitat física o mobilitat reduïda poden optar a beneficiar-se dels serveis que implica aquest equipament, entre ells una residència adaptada. En tot cas, l'usuari del servei ha de signar un contracte de servei residencial com a requisit imprescindible.

En el cas de Sports&Life Guttmann Club, és un servei adreçat no només a antics pacients de l'hospital i a persones del seu entorn, sinó també a qualsevol persona amb una discapacitat d'origen neurològic. Es pretén fomentar la pràctica de l'esport i la realització d'activitats socials i culturals entre persones dels col·lectius esmentats.

A falta de documentació específica per a analitzar, constatem la necessitat de revisar que en els procediments de recollida de dades d'aquests serveis es proporciona la informació sobre el tractament de les dades de conformitat amb l'art. 13 RGPD, bé sigui al contracte, bé sigui a través de qualsevol altre document.

- **Videovigilància:**

A través d'aquesta activitat de tractament es capta la imatge i/o la veu de persones que es troben a les instal·lacions de l'entitat, amb la finalitat de preservar la seguretat i controlar els accessos. Per tant, la base jurídica d'aquest tractament seria el compliment d'una missió en interès públic, d'acord amb l'article 6.1.e) del RGPD.

El tractament el du a terme el servei de vigilància que l'entitat té contractat, l'empresa Ilunion, amb qui l'entitat ja té un contracte d'encàrrec de tractament. Les càmeres es troben instal·lades als corredors, sempre amb finalitat de control d'accessos. No consta que es faci servir mai la videovigilància per a finalitats que no siguin el control de la seguretat.

Durant els treballs de camp podem comprovar que ja hi ha cartells penjats que proporcionen informació sobre el tractament, quan s'accedeix a les zones videovigilades.

D'acord amb la informació proporcionada i el document de seguretat, les dades de videovigilància es van sobreescrivint cada 10-15 dies, en funció de la quantitat d'informació recollida i la memòria disponible.

El tractament descrit és correcte i no planteja problemes de legitimitat o licitud.

- **Investigació.**

La recerca és una activitat rellevant que du a terme l'entitat i constitueix generalment un tractament de dades sensibles o de categoria especial. D'acord amb les informacions proporcionades, l'entitat du a terme diferents activitats de recerca que poden distingir-se entre estudis retrospectius, estudis prospectius i Cohorts. Els estudis retrospectius es duen a terme generalment amb dades seudonimitzades o directament anonimitzades i aquest efecte es demana al Comitè d'Ètica en la Investigació (CEI) una exempció de la necessitat de demanar el consentiment de les persones interessades.

En el cas dels estudis prospectius i el projecte Cohort, el tractament es fonamenta en l'obtenció del consentiment de l'interessat, que pot revocar en qualsevol moment. Els consentiments utilitzats són avaluats sempre pel CEI de forma prèvia i inclouen una informació exhaustiva sobre el tractament de les dades. No obstant, la informació i els consentiments per a la participació en el projecte i el tractament de les dades s'inclouen dins un mateix document. Aquest document és correcte, però, d'acord amb resolucions recents en matèria de recerca per part de les autoritats de protecció de dades, és

recomanable que la informació i el consentiment sobre la participació es proporcioni de forma separada a la informació i el consentiment sobre protecció de dades, com a dos documents diferents.

L'Oficina de Recerca i Innovació és l'encarregada de seudonimitzar. En concret, s'aplica un sistema de codificació sobre l'aplicació que gestiona la història clínica, de manera que se li assigna un número i s'aconsegueix la dissociació efectiva de les dades. En general, per tant, ja hi ha separació tècnica i funcional, perquè només l'investigador principal té la clau per reidentificar, en cas necessari. La resta d'investigadors tracten les dades sense poder identificar en cap cas les persones. No obstant, d'acord amb les informacions proporcionades, no hi ha un compromís de no reidentificació que se'ls faci signar. És important en aquest punt tenir en compte els requisits legals de la seudonimització, segons el model descrit a la disposició addicional dissetena, lletra d), de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades i garantia dels drets digitals, que són:

- Separació tècnica i funcional entre l'equip investigador i els que fan la seudonimització.
- Compromís de confidencialitat i de no fer cap activitat de reidentificació signat per l'equip investigador.
- Aplicació de mesures per evitar la reidentificació.

Tal com podem comprovar, ja s'han dut a terme avaluacions d'impacte per part de l'entitat sobre diferents activitats de tractament de dades. No obstant, no consta que s'hagin dut a terme avaluacions d'impacte sobre projectes de recerca. En aquest sentit, projectes com el Cohort, que implica una recollida massiva i continuada de dades, pot requerir la necessitat de realitzar una avaluació d'impacte. Cal tenir en compte que és obligatòria la realització d'avaluacions d'impacte en relació a tractaments de dades que impliquin un alt nivell de risc per als drets i llibertats de les persones, sobretot si es preveuen elements de monitorització o la introducció de noves tecnologies en el tractament, entre d'altres, de conformitat amb l'art. 35 RGPD i els criteris de la llista de tractaments especificats per l'AEPD. 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. En el cas particular de l'entitat, seria recomanable revisar la necessitat de realitzar una avaluació d'impacte en l'aprovació dels diferents projectes de recerca.

Les autoritats de control han publicat guies sobre criteris i metodologia a emprar en l'elaboració d'avaluacions d'impacte, tant l'Autoritat Catalana de Protecció de Dades (APDCAT) com l'Agència Espanyola de Protecció de Dades (AEPD). També 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. No seria correcte que fos el DPD qui elaborés directament els informes d'avaluació d'impacte, ja que plantejaria problemes de compatibilitat amb les seves altres funcions d'assessorament i supervisió.

- **GNPT**

D'acord amb les informacions i evidències proporcionades, Brain Health Solutions és una empresa participada per GUTTMANN i Grupo ICA per a la comercialització i

manteniment d'una plataforma informàtica dins el sector sòcio-sanitari. El nom d'aquesta plataforma és GNPT i està destinada a tractar dades de pacients. D'acord amb les informacions proporcionades, se signen contractes d'encàrrec de tractament de dades amb els clients, que han estat revisats per la Unió Catalana d'Hospitals. Quan la plataforma es ven a altres centres de salut, l'encarregat del tractament és Brain Health Solutions i el centre de salut actua com a responsable del tractament. En aquest cas, la base jurídica del tractament seria l'existència del contracte de prestació de serveis. Quan el servei es presta als pacients de GUTTMANN, l'entitat actua com a responsable del tractament i Brain Health Solutions com a encarregada. La base jurídica seria, en aquest cas, la mateixa prestació assistencial. D'altra banda, en tots els casos, Grupo Ica actua com a encarregada del tractament.

Constatem que s'ha fet una anàlisi de riscos específica respecte a aquest tractament, la qual s'ha materialitzat en un document i s'ha aportat a aquesta auditoria. D'aquesta manera, s'han tingut en compte riscos i aspectes de licitud, i s'han pogut minimitzar de forma positiva.

D'acord amb les informacions proporcionades, la plataforma disposa d'una intel·ligència artificial i ofereix propostes terapèutiques en relació als pacients. No obstant, tal com matisen els responsables de comercialitzar la plataforma, sempre hi ha un professional humà que pren les decisions. Descartem, per tant, l'existència d'una situació de risc, com podria ser una presa de decisions automatitzada.

Els servidors de la plataforma es troben a Madrid. No consta que hi hagi transferències internacionals contràries al dret.

No es detecten usos de dades que no siguin ajustats a la finalitat o que no estiguin justificats.

- **BBHI - Barcelona Brain Health Initiative**

Aquest tractament no deixa de ser un projecte de recerca que presenta algunes especificitats. Els participants es registren i proporcionen les seves dades a través de la web del projecte, a l'adreça https://bbhi.cat/participa, on han d'emplenar un formulari i llegir necessàriament un primer avís legal sobre el tractament de les dades, que és conforme a l'art. 13 RGPD.

El document de seguretat no indica quina és la base jurídica definida pel responsable del tractament en aquest cas, però resulta clar que és el consentiment del participant, ja que posteriorment a registrar-se haurà d'acceptar expressament una informació sobre el tractament de les dades i tindrà l'opció manifesta de clicar "No hi estic d'acord" i deixar de formar part de l'estudi. El document que ha d'acceptar el participant es diu "*Full d'informació per als voluntaris participants de l'estudi Barcelona Brain Health Iniciative*", que conté també una informació exhaustiva sobre l'estudi, les seves fases i les seves implicacions. En aquest full s'informa a bastament sobre la finalitat del tractament, que en l'anterior avís legal de la web es presentava més difús i poc clar. No obstant, el compliment de l'art. 13 RGPD es feia a través del primer avís legal.

- **Blanqueig de capitals**

Aquest tractament respon a la necessitat legal de conservar les dades de les persones que fan donacions econòmiques, en compliment de la Llei 10/2010, de 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme. Per tant, la base legítima del tractament és el compliment d'una obligació legal. En realitat, més que una activitat de tractament completa, és la conservació d'unes dades obtingudes en una altra activitat de tractament.

Quan els donants són persones físiques, com per exemple els "*Amics de l'Institut Guttmann*", que poden fer donacions a través de la web, seria convenient que s'informés d'aquest tractament en l'avís legal que hi ha al costat del formulari. Ara mateix no es proporciona aquesta informació.

Finalment, cal tenir en compte que el Reial Decret Llei 7/2021, ha modificat la Llei 10/2010 de 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme, de manera que ara aquesta llei estableix al seu article 32 bis, apartat 4, l'obligació de realitzar una avaluació d'impacte sobre aquest tractament de dades. Aquesta obligació afecta tots els subjectes obligats per la llei, entre els quals hi ha les fundacions. En aquest cas concret, ja s'ha documentat l'existència d'un informe d'avaluació d'impacte, però, com a possible millora d'aquest informe i dels altres que s'han documentat, caldria distingir-hi entre el risc inherent (ara no s'hi identifica) i el risc residual, que és el que quedaria com a conseqüència d'aplicar les mesures de seguretat proposades.

Les dades que es conserven són les mínimes imprescindibles, i es mantenen durant el temps de conservació prevista a la llei.

- **Empremtes digitals**

D'acord amb les informacions proporcionades, la dada de l'empremta digital es recull de determinats treballadors per a garantir-ne l'accés a certes zones restringides, com ara el quiròfan, el gimnàs, l'àrea mèdica i l'àrea d'infermeria. La finalitat del tractament, per tant, és garantir la seguretat de determinats accessos. La base jurídica del tractament és la potestat d'organització que correspon a l'empresa.

No consta en la documentació proporcionada que es faci servir un model d'informació sobre l'ús de la dada de l'empremta digital o que hi hagi un procediment de legitimació definit prèviament pel responsable del tractament. Respecte a la darrera auditoria, sí que consta la realització d'un informe d'avaluació d'impacte, que, en tot cas, seria millorable amb els aspectes descrits.

- **Nous tractaments indicats al RAT**

Respecte a la darrera auditoria, comprovem l'existència de noves activitats de tractament identificades al RAT, que revisem en aquest apartat.

- Medxat / AQUAS i Nova HCE

Més que no pas activitats de tractament diferenciades, amb aquests noms s'identifiquen eines informàtiques que s'han implementat a l'entitat i que pretenen facilitar el tractament de la informació corresponent a la prestació assistencial i social. Es constata que s'han identificat al RAT i que se n'ha fet una avaluació d'impacte de forma correcta sobre cadascuna d'elles, si bé els informes són millorables en els aspectes indicats anteriorment sobre el model d'informe.

En qualsevol cas, d'acord amb la informació continguda als informes, aquestes eines han estat descrites i avaluades correctament. No consta que aquestes eines impliquin tractaments de dades desproporcionades o innecessàries, més enllà del que ja s'ha descrit en l'apartat corresponent a la prestació assistencial i social.

- Parking / Cafetería y cocina

Aquestes activitats impliquen tractar les dades necessàries per a la gestió d'aquests serveis del centre Guttmann Barcelona i, per tant, es poden emparar en l'interès legítim de l'entitat i en la gestió d'una subcontractació de serveis.

Les dades tractades són les mínimes imprescindibles per al control i gestió d'aquests serveis i són dades d'un nivell molt bàsic. En el cas de la cafeteria, està gestionada per una empresa concessionària, mentre que el pàrking està gestionat per l'empresa SABA. En tots dos casos, la legitimitat i l'abast dels tractaments es troba definida en els contractes d'encàrrec de tractament de dades, que formen part del procés de contractació amb les entitats gestores dels serveis.

- Estudiantes master, Residentes y Prácticas

A l'entitat hi ha també estudiants, que entren a través d'un conveni amb el corresponent centre de formació i amb l'oferta de pràctiques que hi hagi disponible. En aquest cas, la base jurídica del tractament derivaria del compliment d'aquest conveni. En alguns, és el propi estudiant el que contacta el grup. En qualsevol cas, el procés d'acollida de l'estudiant es realitza en els mateixos termes que es fa el procés d'acollida del personal, tal com s'ha descrit a l'apartat de recursos humans. En qualsevol cas, ja es garanteix que es proporcioni una informació sobre el tractament que és conforme a l'art. 13 RGPD.

No conformitat

▼	Vegeu els comentaris anteriors, especialment les parts subratllades, que són les que fan referència de forma més específica a àrees d'incompliment i millora.

5.7. DRETS DE LES PERSONES INTERESSADES

Base legal: Articles 13-23RGPD

Situació actual

L'entitat disposa dels models i ja té un protocol definit per a l'exercici dels drets de les persones interessades, com es pot comprovar en l'apartat corresponent de tots els documents de seguretat. A l'annex 7 dels documents de seguretat hi ha els diferents formularis i models corresponents als drets d'accés, rectificació, supressió, oposició, limitació i portabilitat. Per tant, ja està previst a l'entitat 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 procediment preveu que el contacte amb el DPD per a l'exercici d'un dret es faci enviant un correu electrònic a protecciodades@guttmann.com.

D'acord amb les informacions proporcionades, a l'àrea d'admissions s'atendrien de forma ordinària peticions d'accés o de rectificació de dades de la història clínica, segons un procediment que garantiria la identitat i el registre, i només en cas necessari es demanaria la intervenció del DPD.

Per ara, no consten procediments d'exercici de drets tramitats formalment segons el procediment determinat pel responsable, si més no d'ençà de la darrera auditoria. En tot cas, el DPD és qui s'encarregaria de gestionar, registrar i contestar aquestes peticions, d'acord amb el procediment previst.

Àrees de millora

●	Caldria disposar d'evidència de quantes peticions d'accés o rectificació es reben anualment a l'àrea d'admissions.

5.8. NOTIFICACIONS DE VIOLACIONS DE SEGURETAT

Base legal: Articles 24 i 33 RGPD

Situació actual

L'entitat aporta evidències i proporciona informació que acrediten l'existència d'un procediment intern de registre d'incidències que es gestiona des de l'àrea de sistemes informàtics. En concret, revisem sis documents que permeten evidenciar l'existència d'un registre amb incidències de seguretat etiquetades amb la categoria "LOPD". El personal coneix l'obligació de comunicar qualsevol incidència a l'àrea de sistemes informàtics. Cada mes, el DPD rep un informe mensual sobre aquestes incidències, que se li envia de forma automatitzada. Tot i que es tracta d'una mesura de seguretat adequada, no garanteix que el DPD tinguin accés puntualment a violacions de seguretat que, d'acord amb la seva gravetat, haurien de ser comunicades a l'autoritat de control en un termini inferior a 72 hores des del moment que l'entitat en va tenir coneixement.

Als documents de seguretat es descriu un procediment relatiu a la comunicació interna, anàlisi i registre d'incidències de seguretat. S'hi descriu també què s'entén per incidència i com s'han de registrar, però no consta documentat un procediment de notificació de violacions de seguretat a l'autoritat de control que correspongui al DPD.

Al document de bones pràctiques que forma part del manual d'acollida i que es proporciona a tot el personal en el moment d'incorporar-se a l'entitat, no hi ha una instrucció sobre clara sobre la necessitat de comunicar al DPD de l'entitat qualsevol incidència o violació de seguretat que tingui a veure amb protecció de dades.

No consta, d'acord amb les informacions proporcionades, que hi hagi hagut fins ara una violació de seguretat que hagi hagut de ser comunicada a l'autoritat de control, en aplicació de l'obligació legal de comunicar violacions de seguretat.

No conformitat

▼	Cal proporcionar per escrit a tot el personal una instrucció específica sobre la seva obligació de comunicar incidències i violacions de seguretat de forma immediata al DPD a través del correu electrònic habilitat. Aquesta instrucció, d'altra banda, hauria de constar entre les instruccions que es donen durant el procés d'acollida del personal al manual de bones pràctiques.

5.9. DIFUSIÓ DE FUNCIONS I OBLIGACIONS

Base legal: Articles 24 i 25 RGPD

Situació actual

D'acord amb les evidències aportades (procediments d'acollida, manuals de bones pràctiques disponibles a la intranet, documents de formació sobre protecció de dades, etc.) l'entitat ja ha realitzat accions de difusió destinades a proporcionar informació i instruccions als treballadors sobre les seves obligacions en matèria de protecció de dades i les mesures de seguretat aplicables.

Tots els procediments d'acollida que se segueixen l'entitat (tant pel que fa a personal laboral, com mercantil, estudiantil o voluntari) preveuen proporcionar per escrit instruccions fonamentals i directrius sobre protecció de dades ja des d'un moment inicial. Aquestes instruccions tenen la consideració de bones pràctiques o codi ètic, segons el procediment d'acollida. Comprovem que el manual de bones pràctiques fa referència a l'antiga LOPD, que ja no és referent, i fa al·lusió a mesures de seguretat previstes pel règim legal d'aquesta llei.

També dins els procediments d'acollida es preveu proporcionar una formació inicial sobre protecció de dades. D'aquesta manera, es garanteix un coneixement fonamental sobre mesures de seguretat, funcions i obligacions del personal en matèria de privacitat i seguretat. Tots aquests documents, d'altra banda, es troben sempre disponibles a la intranet per a tot el personal.

En definitiva, resulta clar que s'estaria complint la necessitat de difondre les obligacions i les mesures de seguretat específiques que tot el personal ha de conèixer i aplicar. Només com a aspecte a millorar, tal com s'ha evidenciat en el punt anterior, caldria incloure al manual de bones pràctiques la necessitat de comunicar qualsevol incidència o violació de seguretat de forma immediata al DPD.

Àrees de millora

●	Seria necessari actualitzar el manual e bones pràctiques que es proporciona al personal en 2 aspectes: - Referències a l'antiga LOPD, que caldria actualitzar. - Incloure-hi l'obligació de tot el personal de notificar qualsevol incidència o violació de seguretat sobre protecció de dades de forma immediata al DPD.

II – BLOC DE MESURES DE SEGURETAT

5.10. DILIGÈNCIES 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

Tant els documents de seguretat de l'entitat com el document "*Annex 17 Sistema de seguretat i pla de contingències*" contenen informació sobre els diferents recursos informàtics que es fan servir a l'organització i els controls que s'apliquen en el seu accés.

Segons les informacions proporcionades i la documentació esmentada, l'entitat ja ha previst la necessitat que l'accés a les dades i recursos del lloc de treball estigui limitat en funció de les responsabilitats laborals de cadascú.

Els entorns informàtics a què ha d'accedir el personal per al tractament de les dades són el domini, el correu electrònic (si és personal intern) i les aplicacions sanitàries, si és el cas. Quan entra un treballador nou a l'entitat, responsables de recursos humans informen al responsable informàtic sobre el perfil d'accés que ha de tenir. Aleshores, se li assigna un nom d'usuari per a cadascun dels entorns diferenciats i una contrasenya provisional, i se li comuniquen en un sobre tancat. En el mateix sobre ja hi ha instruccions per a canviar la contrasenya durant el primer accés. En aquest mateix moment, també se li recull l'empremta digital, que li permetrà fitxar.

En general, les claus d'accés que requereix un treballador són diferents en funció dels entorns d'accés: d'una banda, el domini i el correu electrònic fan servir les mateixes claus. D'altra banda, les aplicacions sanitàries també estan integrades i fan servir unes mateixes claus, que són diferents de les del domini. Finalment, l'aplicació d'INTEGHRO que permet accedir a la pròpia nòmina també requereix una contrasenya diferent, tot i que el nom d'usuari és el mateix del domini.

El nom d'usuari del domini està compost de la primera lletra del nom i el cognom. La contrasenya ha de complir determinats requisits de complexitat (ha de tenir un mínim de 8 caràcters i incloure majúscules i minúscules). Les contrasenyes del domini s'han de renovar necessàriament cada 90 dies. D'altra banda, s'aplica una limitació dels intents d'accés fallits que fa que després 4 intents d'accés fallits es bloquegi la contrasenya. Finalment, també és important tenir en compte que està implementat un sistema de bloqueig per inactivitat com a política de domini, el qual bloqueja l'estació de treball després de 15-20 minuts d'inactivitat.

Pel que fa a les aplicacions sanitàries, el nom d'usuari és alfanumèric, ja que inclou un número que identifica la persona com a professional. La contrasenya també té característiques de robustesa, i ha d'estar formada per un mínim de 8 dígits, entre els quals hi ha d'haver majúscules, minúscules, símbols i números. La renovació obligatòria de la contrasenya es produeix cada 90 dies. D'altra banda, hi ha una mesura de bloqueig per accessos indeguts, que s'activa després de 3 intents fallits, i una mesura de bloqueig per inactivitat, que permet bloquejar l'accés després de 10 minuts de d'absència d'activitat. Val a dir que les aplicacions sanitàries són les corresponents a la gestió de diferents aspectes del servei: curs clínic, admissions, gimnàs, rehabilitació i farmàcia.

Els entorns informàtics disposen d'antivirus de gestió centralitzada i Firewall perimetral que controla les entrades i sortides d'internet.

El document de bones pràctiques que es proporciona al personal inclou mesures de seguretat i control que tot el personal autoritzat a accedir a les dades ha de complir, sobretot en relació als accessos segurs a les dades i al manteniment d'una política adequada de confidencialitat. S'hi preveuen, per exemple, diverses polítiques de control i registre de suports i dispositius que es facin servir per al tractament de dades i una política de pantalla i taula netes.

Per a l'accés físic a les instal·lacions, està previst que només el personal autoritzat pugui accedir als llocs en què es trobin instal·lats els equips físics que donin suport als sistemes d'informació. En general, per a l'accés a determinats espais els membres del personal han de fer servir targetes magnètiques unipersonals, que també els serveixen per fitxar. L'accés a determinades zones restringides també disposa d'un control d'empremta digital.

Els proveïdors externs, per accedir físicament a les instal·lacions, s'han de donar d'alta prèviament en una aplicació de control d'accés, que controla la necessitat de l'accés i emet un passi, que el proveïdor es pot descarregar i que li servirà per poder entrar.

El procediment per a donar de baixa un membre del personal també es realitza a través d'una comunicació per correu electrònic que realitzen responsable de recursos humans al responsable informàtic. Aquesta comunicació sempre té lloc de forma immediata a la modificació o cessament en la prestació de serveis per part d'un treballador. Està previst que en determinats casos determinades baixes siguin temporals. Llavors, l'usuari es manté prudencialment, però deshabilitat i, al cap de 3 mesos, el responsable informàtic pregunta si la baixa temporal ha esdevingut definitiva, a fi i efecte de donar de baixa l'usuari. Un cop l'any els responsables informàtics fan un repàs de tots els usuaris i accessos vigents per confirmar que es corresponen amb la realitat. En general, durant aquesta acció, es repassen sobretot els usuaris deshabilitats per a veure si són definitius.

Pel que fa a les dades més sensibles que tracta l'entitat, les relatives a salut dels pacients i participants dels projectes de recerca, es preveuen mesures de seguretat addicional, com ara el control, registre i revisió periòdica de tots els accessos i intents d'accessos, de què s'aporta evidència. El DPD repassa els informes d'accessos que se li proporcionen des de l'àrea informàtica.

Pel que fa a la documentació en paper, es troba tota desada en despatxos tancats amb clau, dins armaris, ordenada alfabèticament. Es constata, per tant, que 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 troba conservada de forma segura i fora de l'abast d'usuaris no autoritzats. El personal coneix 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.

Finalment, la sala de servidors de Badalona disposa d'accés amb clau, si bé es troba habitualment oberta, mentre que la de Barcelona només és accessible per clau electrònica i/o mecànica.

Àrees de millora

	Com a únic aspecte a millorar, cal destacar la necessitat que la sala de servidors estigui per defecte tancada i no accessible.

5.11. 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 l'entitat per al tractament de les dades es troben degudament actualitzats.

La xarxa informàtica de l'entitat està conformada per diferents ordinadors, servidors i dispositius d'emmagatzematge. El document "Annex 21 Esquema de la xarxa" conté un diagrama de xarxa de l'entitat a Badalona i una relació dels servidors que es fan servir a l'entitat, juntament amb una descripció de la seva ubicació dins les instal·lacions i de les mesures de seguretat que s'hi apliquen.

A banda de disposar d'un Firewall perimetral, que controla les entrades i sortides d'informació, l'entitat també compta amb un antivirus, que escaneja tot el correu electrònic. L'antivirus és de gestió centralitzada i facilita que s'actualitzi en tots els equips.

L'entitat disposa d'un procediment per a l'autorització d'accessos remots als seus sistemes a través de VPN o per DW Service. L'entitat disposa d'un control i registre sobre els usuaris autoritzats. D'altra banda, l'accés remot està protegit per un control d'accés segur que ofereix les mateixes garanties que l'accés ordinari dins les instal·lacions (control d'accés al domini per contrasenya robusta, mesures de bloqueig per intents d'accés fallits i inactivitat, entre d'altres). Per tant, ja s'hi apliquen mesures de control i actualització.

Els equips informàtics no porten bloquejats els ports USB, però el manual de bones pràctiques de l'entitat ja conté instruccions adreçades al personal sobre la necessitat de fer servir unitats de memòria o equips diferents dels previstos per l'organització de forma segura i autoritzada.

No detectada

▲	

5.12. 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 es troba al costat de l'àrea informàtica i només és accessible a través d'aquesta àrea per usuaris autoritzats. Tot i que es pot tancar amb clau, només es tanca durant la nit. Durant el dia, mentre hi ha gent a l'àrea informàtica, ja es garanteix que no s'hi pugui accedir per part d'usuaris que en siguin aliens.

El document "*Annex 17 Sistema de seguretat i pla de contingències*" ja conté una descripció de les mesures de seguretat relatives a l'accés al servidor.

El CPD disposa de tres armaris RACK i diferents mesures de seguretat que s'enumeren a continuació:

- Extintor a l'entrada.
- Sistema d'alarma per detecció de fums.
- Càmera de seguretat.
- Sistema de refrigeració.
- Doble alimentació de corrent elèctric.
- Doble SAI redundats, que podrien garantir el subministrament elèctric durant 10-15 minuts.
- Grup electrogen, que podria proporcionar un corrent alternatiu, en cas necessari.
- Firewall perimetral i antivirus centralitzat.

El CPD disposa d'un SAI, dotat amb un sistema de control de temperatura, que permetria disposar d'un corrent elèctric alternatiu durant vint minuts per al cas improbable d'una interrupció sobtada i imprevista del subministrament ordinari. També hi ha dos grups electrògens, que també podrien proporcionar un subministrament elèctric alternatiu bàsic a l'hospital (només es podria endollar als endolls vermells, que són els considerats bàsics).

No detectada

▲	

5.13. 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

El document "*Manual d'Acollida Guttmann - Versió maig 2022*", que es proporciona al personal en el moment d'incorporar-se a l'organització, conté instruccions de seguretat com a manual de bones pràctiques. Entre aquestes instruccions, ja hi ha instruccions específiques sobre com emmagatzemar dades de caràcter personal en els equips locals o dispositius i sobre com s'han de fer servir de manera responsable determinats suports i dispositius. En particular, els següents punts ja preveuen evitar que es guardin dades en dispositius i que això pugui posar en risc la seguretat de les dades:

9. Els usuaris que gravin documents en el seu disc dur i hagin de fer còpies de seguretat, per raons estrictament professionals, ho hauran de comunicar al departament d'informàtica.

33. Sempre que es faci ús d'un portàtil aliè per fer una presentació o alguna altra feina relacionada o que apareguin dades de pacients, haurem d'esborrar automàticament les dades que haguéssim pogut gravar per efectuar aquest treball.

D'altres previsions del manual de bones pràctiques estableixen l'obligació de registrar les sortides de suports que continguin dades de pacients i la necessitat que les dades de pacients que es trobin en un dispositiu o suport mòbil de qualsevol tipus estiguin xifrades.

No detectada

▲	

5.14. 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

D'acord amb les informacions proporcionades i el document "*Annex 17 Sistema de seguretat i pla de contingències*" ja es preveu l'existència de diferents procediments de còpia de seguretat a tres nivells diferents:

En un primer nivell, es fan còpies a través del software Veam Backup i les gestiona l'empresa externa Gigas. Són còpies de màquines virtuals i de 2 servidors físics. Les còpies són diàries, però el període de retenció és variable segons el servidor. Tota la informació es copia en un servidor del CPD i en un CPD extern propietat de Gigas (es clona).

En un segon nivell, es fan còpies dels servidors en cabines de discos. En aquest nivell, es fan còpies de màquines virtuals i còpies manuals, en previsió que les còpies fetes amb Veam Backup puguin fallar. Els discos es guarden a l'àrea informàtica.

En un tercer nivell, es fan còpies de bases de dades de la història clínica, recursos de xarxa i imatges, que poden ser en discs externs.

Segons un procediment previst, el responsable d'informàtica fa una revisió cada 90 dies per a comprovar l'aplicació correcta de tots els procediments de còpia i recuperació. Segons aquest procediment, es fan proves de recuperació de fitxers.

No detectada

▲	

5.15. 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

En funció de les responsabilitats i funcions 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, els perfils assistencials (personal que s'ocupa del tractament de dades de pacients) tenen un accés a programes assistencials, que, en canvi, no té el personal administratiu. El personal assistencial, per exemple, utilitza les anomenades aplicacions sanitàries, mentre que el personal administratiu no hi té accés.

D'acord amb les informacions proporcionades i el document "*Annex 17 Sistema de seguretat i pla de contingències*", constatem que ja s'han definit diferents perfils d'accés sobre les dades i els permisos que pot tenir el personal a l'hora a l'hora de manipular-les o visualitzar-les. A l'àrea d'enginyeria disposen dels usuaris que tenen un accés autoritzat a les instal·lacions a través de targeta. D'altra banda, a l'àrea d'informàtica disposen de la relació d'usuaris amb accés a dades de caràcter personal i la definició dels seus perfils d'accés. Aquesta relació es manté actualitzada, ja que hi ha procediments d'alta, modificació i baixa d'usuaris que permeten una comunicació entre recursos humans i els responsables informàtics.

En general, tal com comentàvem al punt anterior, és quan s'incorpora una persona nova a l'entitat que s'apliquen uns protocols d'acollida i es defineix el seu perfil d'accés en funció de les dades i recursos a què hagi d'accedir.

No detectada

▲	

5.16. IDENTIFICACIÓ 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

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

En general, el procediment d'alta d'un nou usuari autoritzat de les dades s'acompanya sempre d'un procediment d'acollida en què des de l'àrea de recursos humans es defineixen els accessos i recursos a què ha de tenir accés i n'informa els responsables informàtics perquè ho apliquin. Aquesta informació consta en una relació d'usuaris amb accessos autoritzats. Aleshores, 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, es defineix un nom d'usuari, que consisteix generalment en la inicial del nom + cognom (i si convé, també el segon cognom), que es lliura a l'usuari en un sobre tancat juntament amb una contrasenya provisional i les instruccions per a canviar-la. Fonamentalment hi ha tres entorns informàtics que estan protegits per un mateix tipus de nom d'usuari i contrasenya i que permeten establir diferents perfils d'accés, que són, en primer lloc, el domini i el correu electrònic, que tenen un mateix tipus d'usuari i contrasenya; en segon lloc, les aplicacions assistencials, que estan integrades i també són accessibles a través del mateix tipus d'usuari i de la mateixa contrasenya; i finalment l'accés a la nòmina a través d'INTEGHRO, que també té una contrasenya diferent.

Tal com podem comprovar amb el document "*Annex 17 Sistema de seguretat i pla de contingències*" i tenint en compte les informacions proporcionades, indiquem les diferències i característiques d'aquests diferents tipus d'accés.

Accés al domini i correu electrònic

- Nom Usuari: 1a lletra del nom i cognom
- Contrasenya:
    - Longitud: mínim 8 caràcters.
    - Ha d'incloure majúscules i minúscules
    - S'ha de renovar cada 90 dies.
- Bloqueig per intents d'accés fallits: 4
- Bloqueig per inactivitat: 15-20 minuts.

Accés a les aplicacions sanitàries

- Nom Usuari: Alfanumèric
- Contrasenya:
    - Longitud: mínim 8 caràcters.
    - Ha d'incloure majúscules, minúscules, símbols i números

- S'ha de renovar cada 90 dies.

- Bloqueig per intents d'accés fallits: 3
- Bloqueig per inactivitat: 10 minuts.

En el cas de l'accés a la nòmina a través d'un mòdul del programa INTEGHRO, es fa a través d'una contrasenya sense característiques de robustesa, però que es troba sota la restricció de l'accés al domini.

No detectada

▲	

5.17. ACCESSOS REMOTS

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

Situació actual

L'entitat permet a determinats usuaris, per raons justificades de les seves responsabilitats laborals, que accedeixin remotament als seus sistemes i al tractament de les dades. Només la direcció de l'entitat o el cap de serveis corresponent poden autoritzar un usuari a accedir remotament.

A l'entitat hi ha fonamentalment dos tipus d'accés remots:

1- Per VPN: Aquest accés requereix la configuració d'un accés VPN i està pensat per als que disposen d'estacions de treball segures proporcionades per l'entitat. S'hi apliquen les mateixes mesures de seguretat i control d'accés com si fossin a l'organització.

2- Accés a través de DW Service: Aquest accés es vehicula a través d'un software de connexió remota pensat per a persones que no tenen dispositius de l'entitat i s'han de connectar amb PCs propis. És el sistema que es va fomentar durant la passada pandèmia de Covid-19, però està caient en desús, ja que l'entitat està comprant portàtils per a tot el seu personal. La plataforma de per si ja fa servir usuari i clau per a l'accés remot.

El responsable informàtic manté una relació actualitzada dels usuaris autoritzats a accedir remotament.

A través d'un acord de teletreball, que s'ha proporcionat a tot el personal i que s'ha revisat en aquesta auditoria, es regulen les condicions de teletreball de manera segura, amb un compromís específic de seguretat per part del treballador.

Com a mesura de seguretat rellevant, recordem que hi ha implementada una mesura de bloqueig per inactivitat tant al domini com en les aplicacions assistencials. D'aquesta manera, es minimitza notablement la possibilitat d'accessos indeguts des de fora de les instal·lacions i mitjançant dispositius o equips que escapin al control de l'entitat.

També és important assenyalar que el sistema està protegit per dos Firewalls transversals de Cisco-FTP, en un sistema redundant. Aquest model també s'aplica exactament respecte a la xarxa de Barcelona de l'entitat (amb dos Firewalls més).

No detectada

▲	

5.18. REGISTRE D'ACCESSOS INFORMÀTICS

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

Situació actual

Tal com podem comprovar durant els treballs de camp, s'aplica una mesura de seguretat de registre d'accessos sobre els programes que es fan servir per al tractament de dades de salut. D'acord amb aquesta mesura, el responsable informàtic genera un informe mensual dels accessos als programes assistencials i a la plataforma GNPT. Aquest informe es trasllada al DPD, que el revisa, hi fa propostes de correcció, en cas necessari, i després ho remet a direcció.

S'han a aportat com a evidència 8 documents Excel i pdf corresponents als 5 primers mesos de 2022 que constitueixen evidència de la revisió d'aquests accessos, tant en relació al programa de gestió assistencial com pel que fa la plataforma GNPT. En aquests registres hi consten el PC, el login, el codi d'usuari, la data i l'hora i la història accedida. També és possible visualitzar en aquests registres els accessos que s'han realitzat per perfils.

El procediment previst per l'entitat és correcte i constitueix una garantia que no es produeixin accessos indeguts.

No detectada

▲	

5.19. 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 l'entitat per tractar i conservar dades de caràcter personal ja estan degudament identificats, etiquetats i inventariats. En aquest sentit, totes les màquines, dispositius i suports que es fan servir estan inventariats i duen una etiqueta física, que els identifica.

El document de bones pràctiques que es proporciona al personal, al seu punt 30, estableix l'obligació del personal de fer servir etiquetes:

"*Els suports informàtics que tinguin dades personals, (per exemple: dades de nòmines per les entitats financeres, dades de declaracions tributàries per Hisenda, imatges radiogràfiques, etc.) hauran d'estar clarament identificats amb una etiqueta externa que informi de les da-des contingudes i la data en que es van guardar en el suport informàtic*".

D'acord amb les informacions proporcionades, la mateixa aplicació que es fa servir per a gestionar i registrar les incidències ja inclou l'inventari de suports i dispositius, cosa que permet relacionar-hi les incidències.

El programa GLPI permet fer un inventari actualitzat dels equips i de tot el que porten instal·lat. Amb aquest programa és possible saber els usuaris que accedeixen als equips i vincular-los als diferents departaments.

En tot cas, es porta un control i registre de les persones a qui s'han assignat els equips, suports i dispositius. També es registra quan l'usuari recull o ha de traslladar un dispositiu o suport que conté dades de caràcter sensible.

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

No detectada

▲	

5.20. DESTRUCCIÓ DE SUPORTS

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

Situació actual

El manual de bones pràctiques que s'inclou dins el manual d'acollida ja conté una previsió sobre destrucció de documentació que contingui dades de caràcter personal al seu punt 29:

29. En cas de voler destruir qualsevol document que contingui informació o dades confidencials s'ha de fer necessàriament mitjançant el circuit descrit en el document "Annex 17: Sistema de seguretat informàtic i pla de contingències. Apartat 'Destrucció de discs i papers i protecció de dades".

La instrucció remet a un protocol que conté mesures de seguretat destinades a la destrucció segura de suports. Segons aquest document, ja hi ha un seguit de previsions de destrucció, que comentem a continuació.

D'acord amb les informacions proporcionades i l'Annex 17, que s'ha aportat com a evidència a aquesta auditoria, els discs durs seran formatats quan hagin de ser destruïts o canviats d'ordinador i, per a la seva destrucció física, es desmuntaran i es destruiran fins a esdevenir inservibles. També s'hi preveu que els suports que s'han d'eliminar es sotmetin a processos previs d'esborrat o destrucció, per tal d'impedir-ne una possible recuperació posterior de les dades que s'hi emmagatzemen.

L'entitat disposa d'un procediment específic de baixa de suports, segons el qual el cap de sistemes informàtics ha de signar i autoritzar les baixes per escrit. Llavors, els suports que s'han de donar de baixa es traslladen a l'àrea econòmic-financera; quan hi ha molts discs durs que s'hagin de donar de baixa, el departament d'Infraestructures, Serveis i Medi Ambient (ISMA) s'encarrega que siguin trepanats i que s'enviïn posteriorment a un centre de gestió de residus.

Pel que fa a la documentació confidencial en paper, s'ha de dipositar en una caixa especial destinada específicament a documentació confidencial, que posteriorment acaba destruïda a la trituradora de paper. D'altra banda, als departaments que generen i fan servir documentació en paper, com ara el de recursos humans, disposen d'una màquina trituradora, on poden destruir la documentació que contingui dades de caràcter personal.

No detectada

▲	

5.21. 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'acord amb les instruccions que es proporcionen al personal a través del manual de bones pràctiques, ja hi ha un seguit de previsions i mesures que s'han d'aplicar obligatòriament en la comunicació i sortida de dades; d'entrada, al punt 26 s'estableix la prohibició d'enviar dades de pacients per correu electrònic, a menys que s'hi apliqui algun sistema de xifrat; el punt 32 determina que totes les sortides de suports que continguin dades de caràcter personal hauran de registrar-se en un registre d'entrades i sortides, de conformitat també amb allò establert als documents de seguretat; el punt 34 estableix la necessitat d'encriptar les dades de pacients, sempre que es facin servir dins un dispositiu mòbil; finalment, el punt 45 prohibeix treure històries clíniques fora del centre sense el coneixement i permís del responsable del tractament.

Els documents de seguretat relatius als tractaments de dades sensibles (dades de salut o de recerca) també preveuen mesures d'encriptació per a suports, documents i dispositius que s'hagin de traslladar fora del centre, de manera molt semblant a com ho fa el manual de bones pràctiques. Segons aquests documents, Les dades de pacients que s'envien telemàticament, s'han d'enviar encriptades o dissociades. El departament d'Admissions i Atenció a l'Usuari i l'àrea Mèdica, que son les que tenen més necessitat d'enviar dades de pacients, ho fan amb PDFs xifrats amb AES 128 o AES 256 per substituir els fax. També fan servir el programa Winzip amb xifrat AES 256. Comprovem, en tot cas, que el procediment previst ja preveu que el fitxer s'enviï a través d'una comunicació i la clau a través d'una altra, segons les informacions proporcionades.

No detectada

▲	

5.22. 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, a l'entitat es tracta cada cop menys documentació en paper, però s'apliquen mesures de seguretat en relació a la documentació que encara es fa servir i es conserva.

En general, tota la documentació es troba desada en armaris que sempre estan tancats amb clau i amb accés restringit als responsables del seu tractament autoritzat.

Els espais i despatxos en què es guarda la documentació en paper i els suports informàtics disposen sempre d'un control d'accés físic, com és el cas dels accessos a les instal·lacions i a les oficines. Per a l'accés a aquests espais només es poden fer servir les targetes magnètiques dels treballadors, l'empremta digital per a determinades zones o les claus físiques, en determinats casos. En qualsevol cas, tots aquests espais romanen tancats i restringits, quan no se'n fa ús.

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

No detectada

▲	

5.23 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 paper que es fa servir a l'entitat es troba generalment desada als seus corresponents armaris, situats en despatxos, que es troben sempre tancats, quan no es fan servir. També hi ha un arxiu històric al soterrani. En qualsevol cas, cada cop es conserva menys documentació en paper.

Pel que fa a dades de categoria especial (dades de salut corresponent als projectes de recerca, per exemple), la documentació que es pot arribar a conservar actualment en paper és generalment accessòria o circumstancial, ja que gairebé tota la informació necessària es recull, es tracta i es conserva de forma informatitzada a través de les aplicacions sanitàries corresponents. Segons les informacions proporcionades, no entra ni surt documentació de l'arxiu de forma habitual.

Els documents de seguretat de pacients i investigació estableixen que l'accés a la documentació en paper es limita al personal autoritzat, i es refereixen als documents "*Annex 30 Funcionament de l'arxiu en suport paper*" i "*Annex 27 arxiu històries clíniques*", que s'aplicarien en aquest cas per a la regulació del registre d'accessos. El manual de bones pràctiques que es proporciona al personal estableix al punt 42 que "*tots els membres de l'organització, professionals i col·laboradors, que necessitin consultar les Històries Clíniques en suport paper, hauran d'indicar el seu accés al registre d'entrades i sortides de les Històries Clíniques de l'arxiu corresponent i amb els mecanismes que l'entitat indica en el document de seguretat*".

Respecte a l'arxiu històric d'històries clíniques que hi ha a la planta -2, ja hi ha un procediment previst que s'està aplicant per a l'accés a aquestes històries. Segons aquest procediment, la persona responsable de l'arxiu registraria al programa de gestió de la història clínica que s'ha recuperat la història en paper, i posteriorment en registraria la devolució.

L'entitat ja té mitjans per a la destrucció de documentació confidencial, sobretot màquines trituradores en les àrees que es fa servir documentació en paper. D'acord amb la documentació aportada a aquesta auditoria, hi ha una previsió clara de destruir tota la documentació que tingui dades de caràcter personal a través d'aquest mitjà, la qual cosa ja ha estat també instruïda al personal a través del manual de bones pràctiques.

No detectada

▲	

5.24. 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 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.

Tal com hem comentat als punts anteriors d'aquest informe, la documentació en paper que es pot guardar a l'entitat i que conté dades de categoria especial és residual. En general es guarda documentació del personal, d'administració i de pacients, però la major part de la gestió es du a terme de manera informatitzada.

Pacients: L'única documentació que es guarda encara avui en paper dels pacients és el full d'informació del pacient sobre protecció de dades, el consentiment informat i les proves que només puguin conservar-se en aquest suport documental. Aquests documents es guarden a l'arxiu històric de l'entitat, on també es guarden històries clíniques antigues en paper des del principi de la Fundació. Aquest arxiu es troba en una sala específica de la planta -2, tancada amb clau i només accessible a través de passar per dos accessos que requereixen disposar de dues claus diferents. Només persones de l'àrea d'admissions hi tenen un accés autoritzat, i la persona responsable de l'arxiu i del registre d'accessos és el Sr. Santi Vila. Les històries hi estan ordenades cronològicament i per números. Comprovem durant la visita presencial que l'arxiu disposa d'un extintor a l'entrada, un sistema de detecció de fums i una alarma d'incendis.

Recerca: La documentació que encara es conserva dels participants als projectes de recerca, generalment consentiments informats, es troba emmagatzemada a la sala d'arxiu de la planta -2, ordenada segons la numeració de les històries clíniques. La documentació que encara es pugui fer servir relativa a projectes actuals, es trobaria als despatxos dels investigadors principals, que són els responsables de la seva custòdia.

Personal: Es guarden expedients de tots els treballadors dins armaris tancats amb clau, ordenats alfabèticament, dins els espais de l'àrea de recursos humans i sota la custòdia i supervisió del personal d'aquesta àrea. Cada carpeta té 3 colors, que corresponen als aspectes professional, personal i de formació de la persona. Els contractes es guarden indefinidament, però els justificants es destrueixen al cap de 2 anys. A la sala d'arxiu de la planta -2 s'hi guardaria documentació antiga i passiva de recursos humans des de l'any 1965 sota criteris també alfabètics i cronològics.

Administració: Llevat alguna documentació de facturació residual, que es tractaria a les oficines, la majoria de documentació en paper es troba a l'arxiu del soterrani, on es conserva per períodes de 4 anys (documentació fiscal), 6 anys (documentació legal) i 15 anys (subvencions).

Externs: La documentació i expedients dels estudiants es troba desada i ordenada a l'àrea de docència segons cursos acadèmics i número de matrícula. Així mateix, s'organitzen en diferents carpetes segons sigui MIR, pràctiques, postgrau o Màster. El passiu es guarda al mateix

departament, amb documentació que es remunta a 20 anys enrere. La responsable de l'arxiu és la coordinadora de docència.

Treball Social: La documentació que es fa signar als voluntaris i la que es genera dels treballs en benefici de la comunitat es troba emmagatzemada als despatxos de l'àrea de treball social, ordenada per departaments, serveis i dates, sense diferenciar distingir l'actiu del passiu. La documentació es guarda de manera indefinida. La persona responsable d'aquest arxiu seria la mateixa cap de treball social.

Reclamacions i atenció a l'usuari: La documentació relativa als procediments de reclamació i suggeriment de pacients està desada a l'àrea d'Admissions. El criteri d'arxiu és per anys. La responsable de l'arxiu és la cap de Departament d'Admissions.

Àrees de millora

●	Tot i que s'apliquen polítiques de destrucció de documentació antiga en alguns àmbits, no és així en les àrees de recursos humans i pacients, on es conserva tota la documentació en paper des del principi. En aquest sentit, caldria aplicar criteris i terminis de conservació i dur a terme accions de destrucció antiga, quan aquesta documentació ja no sigui necessària i ja no estigui justificada la seva conservació.

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. 5.3. Definició de les mesures de seguretat per part del responsable del tractament. 5.5. Encarregats del tractament i proveïdors sense accés a dades. 5.7. Drets de les persones interessades. 5.9. Difusió de funcions i obligacions del personal.
II – BLOC DE MESURES DE SEGURETAT
5.10. Diligències dels accessos. 5.24. Criteris d'arxiu.
NO CONFORMITAT
I – BLOC GENERAL
5.6. Licitud del tractament, base jurídica, informació i consentiment.
5.8. Notificacions de violacions de seguretat.

Barcelona, 4 de juliol de 2022

Pere Ruiz Espinós

- Soci -

Caterina Bartrons Pou

- Gerent -