Institut Guttmann

Protecció de dades de caràcter personal

Febrer de 2025
Protocol C-18.445

FUNDACIÓ INSTITUT GUTTMANN

Informe d'Auditoria de protecció de dades de caràcter personal

ÍNDEX

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 pseudonimització), 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.

2. METODOLOGIA

Per a portar a terme l'auditoria s'han realitzat entrevistes telemàtiques i algunes revisions *in situ* de les instal·lacions de tractament de dades i sistemes d'informació de l'entitat.

Tant la planificació com els treballs 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, a més dels legals.

Per a 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 revisat i avaluat les següents àrees de l'entitat:

- Delegat de protecció de dades
- Sistemes d'informació
- Centre de processament de dades
- Infraestructures, serveis i medi ambient (ISMA)
- Prevenció de riscos laborals
- Videovigilància
- Recursos humans
- Comunicació i responsabilitat social corporativa
- Recerca i innovació
- Guttmann Neuropersonal Trainer (GNPT)
- Admissions i atenció al pacient
- Àrea mèdica
- Treball social (programa de voluntariat)
- Infermeria
- Rehabilitació funcional
- Neuropsicologia
- Àrea econòmica i financera
- Guttmann Barcelona: Institut de Salut Cerebral i Neurorehabilitació i Guttmann Barcelona Life
- Admissions i atenció al pacient de Guttmann Barcelona
- Apartaments de Guttmann Barcelona Life

Els treballs d'auditoria s'han dut a terme de forma presencial i s'han revisat especialment el centre de processament de dades (CPD) i els espais físics de Gutmann Barcelona: l'Institut de Salut Cerebral i Neurorehabilitació i els apartaments de Gutmman Barcelona Life.

3.2.1. Dates de les fases de realització de l'auditoria

Data dels treballs d'auditoria	28 i 29 de novembre de 2024
Data de l'emissió de l'informe	12 de desembre de 2024

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. Miguel Riazuelo	Responsable de medi ambient i emergències
2	Sr. Javier Remacha	Cap de l'oficina tècnica de gerència i delegat de protecció de dades (DPD)
3	Sra. Sara Rojano	Tècnica en l'àmbit jurídic
4	Sr. Roger Marsal	Cap de sistemes d'informació
5	Sra. Sílvia Calvo	Cap d'infraestructures, serveis i medi ambient (ISMA)
6	Sra. Sheila Patricio	Responsable de prevenció de riscos laborals
7	Sra. Elisenda Bassas	Cap de recursos humans
8	Sra. Sandra Palomo	Adjunta de recursos humans
9	Sra. Elisabet González	Cap de comunicació
10	Sra. Emma Cots	Tècnica de comunicació
11	Sra. Natàlia Jurado	Tècnica de comunicació
12	Sr. Javier Solana	Director de recerca
13	Sr. Eloi Opisso	Director d'innovació
14	Sr. David Hurtado	Responsable de màrqueting del GNPT
15	Sr. Sergi Pedraza	Cap d'admissions i atenció al pacient
16	Dr. Jesús Benito	Metge adjunt
17	Sra. Àngels Hervás	Cap de l'àrea de treball social
18	Sra. Laura Pla	Responsable de voluntariat
19	Sra. Eulàlia Castillo	Supervisora general d'infermeria de l'hospital
20	Sr. Ignasi Soriano	Adjunt a rehabilitació
21	Sra. Antònia Enseñat	Cap de neuropsicologia
22	Sr. Hèctor López	Cap de l'àrea econòmica i financera
23	Sr. Jordi Camps	Responsable de manteniment a Guttmann Barcelona
24	Sra. Meritxell Ruiz	Cap d'admissions i atenció al pacient a Guttmann Barcelona
25	Sra. Marta Sans	Responsable dels apartaments a Guttmann Barcelona

Relació de la documentació lliurada a l'auditor:

- Menú documentació auditoria 2024.
- Registre Activitats del Tractament IG 2024.
- Sol·licitud Inscripció DPD Maig 2018.
- Formulari de nomenament de DPD Institut Guttmann maig 2018.
- Annex 17 Sistema de seguretat i pla de contingències.
- Annex 21 Esquema de la xarxa.
- Pla de Protecció de Dades Personals 2023-2025.
- Autorització Pacient per al Tractament de Dades.
- Autorització Gravació Sessions Formatives.
- Autorització Presa d'Imatge i Veu.
- Autorització presa d'imatges i veu per part del representant legal.
- Annex 19 model contracte ET.
- Contractes d'encàrrec de tractament de dades: Canon Medical Systems, S.A. (manteniment dels ecògrafs i reparació dels equips), MRW Badalona Courier, S.L. (serveis de missatgeria), BTS S.p.A. (sistema de captura de moviment), Zemsania, S.L., Patricio Martínez Maximia Torruella Arquitectura, S.L. (assistència en serveis de projectes i obres d'arquitectura i accessibilitat).
- Acords de confidencialitat: Fundació iSocial (gestió de la justificació econòmica i tècnica) i Josep Maria Escartín (auditor-censor de comptes col·legiat).
- Mostra d'informes mensuals d'incidències registrades de gener a juliol de 2024.
- Mostra d'informes mensuals de registres d'accessos a històries clíniques de gener a setembre de 2024.
- Mostra d'informes mensuals d'accions relatives al GNPT Brain Health Solutions de gener a setembre de 2024.
- Consentiment informat template (recerca).
- Guia d'elaboració de projectes 2024 (recerca).
- Plantilla full informatiu (recerca).
- Qüestionari consentiment informat (recerca).
- Revisió mèdica (comunicació al treballador/a sobre reconeixements mèdics específics).
- Contracte GNPT Brain Health Solutions.
- Annex 07_1 Formulari dret ACCÉS ca.
- Annex 07_1 Formulari dret RECTIFICACIÓ ca.
- Annex 07_1 Formulari dret SUPRESSIÓ ca.
- Annex 07_1 Formulari dret PORTABILITAT ca.
- Annex 07_1 Formulari dret LIMITACIÓ ca.
- Annex 07_1 Formulari dret OPOSICIÓ ca.
- Anàlisis de riscos 2024.

- Avaluació d'Impacte Servei Idonia.
- Informe auditoria 2022 Guttmann.
- Informe control de qualitat Guttmann.
- Constància documental conclusions auditoria.
- Document d'informació i compromís del professional
- Compromís de voluntariat
- Annex 39 Protocol de bones pràctiques amb les dades de caràcter personal 2024_0304
- Manual Acollida Guttmann Digital

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 d'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.

D'acord amb les informacions i evidències proporcionades, l'entitat ja té implementada una política de realització biennal d'auditories sobre protecció de dades.

La darrera auditoria, tal com podem comprovar, es va fer l'any 2022, i va donar com a resultat un informe que porta data de 04/07/2022 i del qual s'ha aportat evidència. No obstant, no consta que el resultat d'aquest informe s'hagi comunicat a la direcció de l'entitat.

Consten evidències d'haver-se fet un control de qualitat sobre protecció de dades l'any 2023 i d'haver-se donat trasllat i informat el resultat d'aquest informe al Comitè de Direcció el 12/09/2023, tal com podem comprovar amb les evidències aportades.

Per tot plegat, podem constatar que ja s'està aplicant correctament una mesura de seguretat de realització d'auditories biennals i que ja s'informen correctament a la direcció de l'entitat, de forma documentada.

Àrees de millora

●	Tot i que s'ha aportat com a evidencia l'informe d'auditoria, l'informe de control de qualitat sobre protecció de dades i l'acta en què s'informa al Comitè de Direcció sobre el resultat del control de qualitat, caldria una major evidència que el resultat de l'auditoria es va informar també al Comitè de Direcció i que com a conseqüència d'aquesta informació es van adoptar mesures correctores.

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 les dades de salut de les persones ateses. Per tant, en aplicació de les previsions del RGPD, l'entitat està obligada a elaborar i mantenir un RAT.

A data de l'auditoria, l'entitat manifesta i pot evidenciar que ha elaborat un RAT, de què constatem l'evidència documental en un document Excel, el qual conté identificats els següents tractaments de dades:

- Pacients
- Personal
- Administració
- Reclamacions
- Externs RRPP
- Externs Amics
- Videos Formació
- Externs Guttmann Barcelona Life
- Externs Sports & Life Guttmann Club
- Externs Docència
- Externs Voluntaris
- Externs TBC
- Vídeo Vigilància
- Investigació
- GNPT
- BBHI
- Prevenció del blanqueig de capitals
- Empremtes Digitals Àrea Mèdica
- Medxat
- AQUAS
- Nova HCE
- Parking
- Cafeteria i cuina
- Estudiants màster, residents i personal en pràctiques
- Registre assistència pacients

Es comprova que els models utilitzats per a l'elaboració del RAT ja contenen efectivament emplenats tots els camps previstos per l'article 30 RGPD (finalitats del tractament, categories de dades, terminis o criteris de supressió, destinataris de les dades, etc.), descrits de forma correcta, i que contenen informacions addicionals, com ara les bases jurídiques aplicables. També incorporen en molts casos una anàlisi de riscos i de la necessitat de dur a terme una avaluació d'impacte i/o una anàlisi del compliment dels principis de privacitat des del disseny i per defecte.

D'entre tots els tractaments identificats al RAT, n'hi ha dos que es fan com a encàrrec del tractament: Treballadors en Benefici de la Comunicat (TBC), que identifica el Departament de Justícia com a responsable del tractament, i AQUAS, que identifica l'HC3 com a responsable del tractament. Cal revisar que aquests tractaments, que responen realment a un conveni i a una regulació de caràcter públic, es duen a terme realment com a encàrrec del tractament. A aquest efecte, pel que fa als TBC, cal revisar el conveni amb el Departament de Justícia, que és el que ha de definir com es du a terme el tractament de les dades. En el cas de l'HC3, el tractament es du a terme com a responsable del tractament.

Com a novetat respecte a la darrera auditoria, s'ha incorporat un tractament de dades de registre d'assistència de pacients a Guttmann Barcelona.

Durant els treballs de camp, es detecten alguns tractaments de dades que probablement no es troben correctament reflectits en el RAT actual i que s'hi haurien de reflectir. En particular, caldria valorar la incorporació al RAT dels següents tractaments:

- Usuaris de la web Siidon – L'existència d'aquestes dades implica un tractament diferenciat, que es podria incloure com a part d'un tractament més genèric de dades de comunicació.
- Canal de denúncies – L'existència d'un tractament de dades vinculat al canal de denúncies implica un tractament de dades diferenciat que s'hauria de reflectir també al RAT.
- Visitants de Guttmann Barcelona – L'existència d'un registre de visitants a Guttmann Barcelona (diferent del registre d'assistència de pacients) implica un tractament de dades diferenciat.

D'acord amb la disposició final onzena de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (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

●	Cal revisar que els tractaments que, segons el RAT, es duen a terme com a encàrrec del tractament (TBC i AQUAS) no es duguin a terme realment com a responsable. A aquest efecte, cal revisar que no hi hagi un contracte d'encàrrec de tractament o una atribució específica de l'administració que atribueixi a l'entitat la condició d'encarregada del tractament respecte a aquests tractament, ja que altrament el tractament es durà a terme amb l'entitat com a responsable. Com a millora, cal valorar la incorporació al RAT dels tractaments de dades detectats durant els treballs de camp, tal com s'ha indicat.

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

Base legal: Articles 24, 25 i 32 RGPD

Situació actual

L'entitat ha elaborat diferents protocols i documents que contribueixen a la descripció de la política de seguretat del responsable del tractament, amb indicació de processos i de mesures de seguretat específiques. Aquests documents contenen previsions adoptades per l'entitat en matèria de protecció de dades i s'han aportat com a evidència. En particular, són els següents documents:

- Annex 17 Sistema de seguretat i pla de contingències.
- Annex 21 Esquema de la xarxa.
- Pla de Protecció de Dades Personals 2023-2025.

Constatem també particularment l'evidència d'unes instruccions sobre seguretat proporcionades al personal, com ara el document "*Annex 39 Protocol de bones pràctiques amb les dades de caràcter personal 2024_0304*" (protocol de bones pràctiques), el qual ja preveu un règim sancionador per al cas d'incompliment. També podem comprovar l'existència d'una previsió de formació a tot el personal, segons la qual tot el personal ha de fer un curs anual online sobre protecció de dades. No obstant, a la pràctica, no és obligatori i només un 70% aproximat de la plantilla l'ha estat cursant.

Algunes de les mesures adoptades per l'entitat, tal com podem corroborar amb la documentació i informacions proporcionades, 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 vàlides. El RGPD no impedeix que les mesures de seguretat previstes pel RLOPD continuïn aplicant-se a fi 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. En aquest sentit, 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 en termes generals 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 s'hi durà a terme un registre d'accés.
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 profusament en diferents punts d'aquest informe.

És important tenir present la Sentència del Tribunal Suprem 188/2022 de 15 de febrer, en què el tribunal considera les mesures de seguretat en protecció de dades com a una obligació de mitjans i no de resultat. Per tant, l'entitat ha d'acreditar que les mesures s'han implementat segons l'estat de la tecnologia de cada moment, per tal d'aconseguir el resultat esperat amb els mitjans adequats i suficients i no pel resultat produït. A més, es tracta no només de dissenyar mitjans tècnics i organitzatius i implementar mesures de seguretat, sinó d'establir mecanismes de control, disposar d'una cultura de seguretat i realitzar controls i proves per a verificar la seguretat de les mesures.

Els tractaments que realitza l'entitat a data de l'auditoria són, en gran part, 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.

Els diferents documents elaborats per l'entitat preveuen polítiques de seguretat i contenen una descripció de com es tracten les dades en les diferents activitats de tractament que du a terme a l'entitat i de les mesures de seguretat que està previst aplicar-hi. Del seu contingut pot inferir-se també que l'entitat ha analitzat i tingut en compte riscos del tractament, sobretot els derivats d'accessos i usos indeguts.

En termes generals, tenint en compte globalment els processos i mesures de seguretat que s'apliquen a l'entitat, podem confirmar que s'apliquen els principis de la privacitat en el disseny i per defecte.

Segons informacions i evidències proporcionades, ja s'haurien fet accions específiques d'anàlisis del risc, que s'haurien documentat en el mateix RAT i en el document Excel "*Anàlisis de riscos 2024*", aportat a aquesta auditoria com a evidència. Aquest document ja està actualitzat i inclou una anàlisi dels riscos tenint en compte la seva probabilitat i l'impacte.

Segons l'evidència aportada, d'ençà de la darrera auditoria ja s'ha fet un informe d'avaluació d'impacte sobre l'ús d'un software de gestió d'imatges i informes mèdics (aplicació Idonia). Aquesta avaluació d'impacte l'ha dut a terme una empresa externa el passat 29/12/2023.

Durant els treballs de camp, detectem l'ús de noves tecnologies sobre les quals no sempre queda acreditat si se n'ha analitzat el risc i la necessitat de fer-ne una avaluació d'impacte: l'ús de Medxat per a videoconsulta, la implementació de la nova història clínica, el sistema de reconeixement facial de pacients a Guttmann Barcelona, l'ús de l'empremta digital dels treballadors per al fitxatge i/o accés a espais restringits, entre d'altres. En particular, el sistema de reconeixement facial, pels riscos que pot implicar, requereix molt probablement una avaluació d'impacte.

A partir de les entrevistes realitzades, no consta que es faci algun ús de la intel·ligència artificial (IA) en el tractament de les dades personals. No obstant, caldria revisar periòdicament la possible implementació de tecnologies que facin ús de la IA i que impliquin algun tractament de dades.

Àrees de millora

●	Constatem en termes generals l'existència d'una gestió proactiva del risc, que es manifesta en les anàlisis de risc documentades en el RAT i en el document Excel aportat com a evidència. En el cas de la formació al personal sobre protecció de dades, cal assegurar que és obligatòria per a tota la plantilla (i no només un 70%) i cal poder guardar evidència del seu seguiment i avaluació. La implementació de noves tecnologies en el tractament de dades de categoria especial (dades de salut, entre d'altres) implica en molts casos la necessitat de dur a terme avaluacions d'impacte. En particular, les tecnologies que poden requerir dur a terme avaluacions d'impacte i la seva actualització periòdica posterior, tal com hem pogut detectar durant els treballs de camp, són les següents: • Ús de Medxat per a videoconsultala • Implementació de la nova història clínica • Sistema de reconeixement facial de pacients a Guttmann Barcelona • Ús de l'empremta digital dels treballadors per al fitxatge i/o accés a espais restringits És necessari revisar la necessitat de dur a terme una avaluació d'impacte o la seva actualització en els casos indicats. Finalment, és important tenir en compte periòdicament l'aplicació de mesures de seguretat i els riscos que pot implicar la possible implementació de tecnologies que facin ús de la IA tant en les accions de formació com en les anàlisis de riscos.

5.4. DELEGAT DE PROTECCIÓ DE DADES

Base legal: Article 37 RGPD

Segons la informació i evidències proporcionades, l'entitat va nomenar el Sr,. Javier Remacha Fuentes com a delegat de protecció de dades (DPD). Aquest nomenament es va notificar posteriorment a l'APDCAT en data 01/05/2018, tal com podem comprovar amb l'evidència documental aportada. L'APDCAT va notificar la recepció de la comunicació el mateix dia i va certificar posteriorment la inclusió del DPD en la seva base de dades. Tal com podem comprovar, el DPD ja consta com a registrat a la base de dades pública sobre delegats de protecció de dades de l'APDCAT i ja hi consta específicament el seu correu de contacte protecciodades@guttmann.com.

La figura del DPD també consta en l'organigrama de l'entitat per sota de la direcció; d'aquesta manera, el personal pot conèixer l'existència d'aquesta figura.

El DPD té coneixements i formació sobre protecció de dades. De forma particular, ha rebut formació específica de la Fundació Unió Catalana d'Hospitals i ha assistit a sessions específiques. També va un curs a AENOR sobre protecció de dades. El DPD, que també és cap de l'oficina tècnica de gerència, du a terme altres tasques sobre prevenció de riscos laborals, responsabilitat social corporativa, projectes, qualitat i assessorament legal. Per tant, el càrrec de DPD és intern, compatible i sense conflicte d'interès.

Com a forma de reportar a direcció, el DPD es reuneix cada dues setmanes amb la direcció de l'entitat per a despatxar afers relatius a l'oficina tècnica i protecció de dades.

No consta que hi hagi a l'entitat una comissió específica de protecció de dades.

Sota la coordinació del DPD s'han dut a terme diferents accions de formació sobre protecció de dades al personal. En particular, s'ha promogut un curs que tot el personal ha de fer online de forma anual.

Entre les tasques que du a terme el DPD hi ha l'atenció dels drets dels interessats, la resolució de consultes, la revisió de possibles accessos indeguts, la promoció de contractes d'encàrrec de tractament de dades, l'assessorament del comitè de direcció i la coordinació de la formació sobre protecció de dades. El DPD és la persona encarregada de dur a terme les comunicacions amb l'autoritat de control en cas de notificació de violacions de seguretat o altres qüestions procedimentals relatives amb aquesta institució.

Confirmem que, en termes generals, els textos legals que fa servir l'entitat per a informar sobre un tractament de dades, de conformitat amb l'art. 13 RGPD, ja informen també sobre l'existència de la figura de la DPD i la possibilitat de comunicar-s'hi a través d'un correu electrònic específic.

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

Segons les informacions i evidències aportades, l'entitat ja du a terme un control i seguiment de les persones o empreses externes a qui permet un accés autoritzat a les seves dades, i té signats contractes d'encàrrec de tractament amb totes elles. Es constata l'existència d'un model de contracte ajustat a la normativa ("*Annex 14 Model contracte ET*"), que l'entitat fa signar.

Tal com podem comprovar durant els treballs de camp i, segons les evidències aportades, ja hi ha un document Excel centralitzat amb el registre de tots els contractes, de manera que se'n pot fer un control i seguiment. No consta que hi hagi un protocol específic sobre gestió d'encarregats del tractament.

Els contractes d'encàrrec de tractament signats que s'han aportat a aquesta auditoria com a mostra per a la seva revisió són ajustats al RGPD i estan actualitzats, en termes generals.

Un cop revisada la mostra aportada de contractes d'encàrrec de tractament de dades personals, fem els següents comentaris al respecte, en cas necessari:

ETs DETECTATS	SERVEI PRESTAT	CONTRACTE
Canon Medical Systems, S.A.	Manteniment dels ecògrafs i reparació dels equips	✓
MRW Badalona Courier, S.L.	Serveis de missatgeria	✓
BTS S.p.A.	Sistema de captura de moviments	✓
Zemsania, S.L.	El contracte no defineix els serveis prestats de forma adequada	✗
Patricio Martínez Maximia Torruella Arquitectura, S.L.	Assistència en serveis de projectes i obres d'arquitectura i accessibilitat	✓

Recordem també que el dia 25/05/2022 va expirar el termini de moratòria per a l'actualització al RGPD de contractes d'encàrrec de tractament de durada indefinida. Per tant, d'ençà d'aquest moment tots els contractes que encara estiguin signats sota el règim legal anterior al RGPD no poden considerar-se vàlids.

No consten contractes que estiguin signats sota el règim legal anterior al RGPD entre la mostra de contractes aportats.

No consta que s'estiguin aplicant mesures específiques de verificació que els encarregats de tractament compleixin les indicacions del responsable del tractament o siguin requerits per a l'aportació d'informació sobre l'aplicació de mesures de seguretat i confidencialitat.

No hi ha entre la mostra de contractes aportats exemples de contractes en què sigui l'entitat la que exerceixi funcions d'encarregada del tractament. Tanmateix, segons informacions proporcionades, l'entitat fa servir el mateix model de contracte d'encàrrec de tractament de dades per a aquests casos, invertint-hi els rols de l'encàrrec.

Àrees de millora

●	Cal incloure en els contractes d'encàrrec de tractament una definició del servei prestat pel proveïdor, el qual justifica i defineix l'accés a les dades. De forma particular, cal esmenar el contracte amb Zemsania en aquest sentit. És important aplicar mesures de verificació que els encarregats de tractament apliquen mesures de seguretat i confidencialitat i compleixen les indicacions del responsable del tractament. En aquest sentit, és recomanable disposar d'un protocol específic per a regular la selecció i relació amb encarregats del tractament.

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. A fi de prevenir aquesta situació de risc i un possible accés indegut, correspon aplicar un compromís de confidencialitat.

Tal com podem comprovar amb l'evidència aportada, l'entitat ja té la previsió de fer signar un compromís de confidencialitat a proveïdors externs que no hagin de tenir cap accés autoritzat a les dades. Aquest compromís s'inclou en les regulacions contractuals amb determinats proveïdors i és ajustat a la normativa vigent sobre protecció de dades.

Un cop revisada la mostra aportada de compromisos de confidencialitat signats, fem els següents comentaris al respecte, en cas necessari:

PROVEÏDORS	SERVEI PRESTAT	COMPROMÍS
Fundació iSocial	Gestió de la justificació econòmica i tècnica	✓
Josep Maria Escartín	Auditor-censor de comptes col·legiat	✓

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

S'analitza a continuació la legitimitat de les activitats de tractament de dades que du a terme l'entitat. A aquest efecte, analitzem els diferents tractaments identificats al RAT, que són els següents:

- ✓ Pacients
- ✓ Personal
- ✓ Administració
- ✓ Reclamacions
- ✓ Externs RRPP
- ✓ Externs Amics
- ✓ Videos Formació
- ✓ Externs Guttmann Barcelona Life
- ✓ Externs Sports & Life Guttmann Club
- ✓ Externs Docència
- ✓ Externs Voluntaris
- ✓ Externs TBC
- ✓ Vídeo Vigilància
- ✓ Investigació
- ✓ GNPT
- ✓ BBHI
- ✓ Prevenció del blanqueig de capitals
- ✓ Empremtes Digitals Àrea Mèdica
- ✓ Medxat
- ✓ AQUAS
- ✓ Nova HCE
- ✓ Pàrquing
- ✓ Cafeteria i cuina
- ✓ Estudiants màster, residents i personal en pràctiques
- ✓ Registre assistència pacients

- **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.

En general, les dades dels pacients poden obtenir-se a través de procediments de derivació (hospitals d'aguts i centres d'atenció primària, sobretot), però poden completar-se amb dades del registre central d'assegurats (RCA) o que proporcionin els mateixos pacients. De forma ordinària, la derivació comença amb un correu electrònic. Aleshores, la persona s'incorpora al programa de pacients, s'avalua el seu informe de derivació i, si es confirma que pot ser admès, se'l trasllada a l'hospital o se'n gestiona la seva citació i trasllat. Quan el pacient és present per primer cop a l'hospital, se li proporciona un full d'informació sobre protecció de dades, del qual s'ha aportat evidència. Aquest document ja conté tota la informació sobre el tractament de les seves dades, de conformitat amb l'art. 13 del RGPD. Val a dir que, en alguns casos, aquest full es proporciona amb anterioritat a la seva incorporació a l'hospital, amb la idea que el porti ja signat de casa seva. El servei d'atenció al pacient és ordinàriament el servei responsable de vetllar perquè el pacient signi el full de protecció de dades. D'altra banda, el DPD manté sempre un control sobre si els pacients han rebut i signat el full de protecció de dades.

El full d'informació del pacient (el document *Autorització Pacient per al Tractament de Dades*") permet també autoritzar opcionalment un seguit de tractaments de les dades addicionals. Aquests usos de les dades, que l'entitat pretén realitzar amb el consentiment exprés i previ 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 d'un model d'autorització, el qual permet prestar el consentiment exprés i inequívoc per a l'ús de la imatge, de conformitat amb el RGPD.

D'altra banda, en relació al tractament de dades assistencials, cal tenir present que l'adopció de noves tecnologies per al tractament de dades, especialment en el tractament de dades de categoria especial, pot requerir la necessitat de dur a terme avaluacions d'impacte. En aquest sentit, tal com hem comentat anteriorment en aquest informe, cal tenir en compte

els usos de Medxat, del gestor de la història clínica i del sistema de reconeixement facial implementat a Guttmann Barcelona, els quals poden requerir la realització d'una avaluació d'impacte.

- **Personal**

En general, aquests tractaments responen a les necessitats de gestió de relacions laborals i a l'organització dels recursos humans a l'entitat. La base jurídica que permet el tractament de les dades es fonamenta en la preparació i execució d'un contracte de treball, de conformitat amb l'article 6.1.b) del RGPD. En el cas de la prevenció de riscos, la vigilància de la salut (salut laboral) i la formació al personal laboral, la legitimitat del tractament també deriva del compliment d'una obligació legal, d'acord amb l'article 6.1.c) RGPD.

De forma general, la selecció de personal, la contractació, l'elaboració de les nòmines i la gestió de recursos humans es du a terme internament. Els treballadors poden accedir a la seva nòmina a través del Portal de l'Empleat, que és un mòdul de l'entorn INTEGRHO. D'altra banda, hi ha alguns aspectes de la relació laboral que es poden gestionar a través de l'aplicació BOLT, com ara les vacances, els permisos, el calendari, els torns, etc.

Per al control de presència i registre de jornada, l'entitat té implementat un sistema de fitxatge per empremta digital. Si bé l'ús de l'empremta digital no és obligatori i, de fet, es pot fitxar alternativament amb la targeta, cal tenir en compte que aquest sistema no s'ajusta al criteri actual d'interpretació del RGPD expressat per les autoritats de control i podria ser objecte de sanció. La Directriu del Comitè Europeu de Protecció de Dades (26/04/2023) considera que les dades necessàries per al reconeixement facial o la dada de l'empremta digital són dades especialment sensibles, i prohibeix l'ús de l'empremta digital com a mètode de fitxatge a les empreses. En el mateix sentit s'ha pronunciat l'AEPD en la seva "*Guia sobre Tractaments de Control de Presència mitjançant Mitjans Biomètrics*". Per tant, aquest ús es considera il·lícit i pot ser considerat mereixedor de sanció. Una altra cosa és l'ús de l'empremta digital per al control d'accés a determinats espais restringits, el qual pot estar justificat.

Tot el personal de l'entitat disposa d'una targeta identificativa, la qual es fa servir amb 2 finalitats:

- Reconeixement i identificació del treballador per a l'accés a espais restringits (quiròfan, vestuaris, etc.)

- Fitxatge, en alguns casos

A l'entitat es duen a terme processos de selecció de personal des l'àrea de recursos humans; en general, l'entitat disposa d'una borsa de treball amb personal de pràctiques. És imprescindible en aquest punt recordar que, si les dades del personal de pràctiques s'incorporen en una borsa de treball cal informar-ho prèviament en la informació sobre protecció de dades que es dona a aquest personal. Per a la cobertura de llocs de treball de personal mèdic, es posen anuncis en col·legis professionals o a través de les aplicacions

d'Infojobs i LinkedIn. També es poden rebre currículums a les àrees d'infermeria o rehabilitació directament, perquè ells farien els processos de selecció corresponents. A l'àrea de recursos humans es duen a terme els processos de selecció del personal administratiu. A la web de l'entitat hi ha un apartat "*Treballa amb nosaltres*", a través del qual un candidat pot enviar la seva informació per a participar en un procés de selecció. El procés d'inscripció com a candidat en les ofertes publicades en aquest apartat de la web ja implica accedir necessàriament a la informació sobre el tractament de les dades. No consta que hi hagi currículms en paper. El període previst de conservació de currículums és d'un any.

Durant el procés d'acollida d'un nou membre del personal, segons una previsió ja definida, es proporciona a la nova persona diferents documents, que són:

- ✓ Document d'informació sobre protecció de dades i compromís de confidencialitat
- ✓ Manual d'acollida per a professionals
- ✓ Protocol de bones pràctiques
- ✓ Codi Ètic i Codi de Conducta
- ✓ Formació obligatòria inicial

Tal com podem comprovar en els models documentals indicats, que hem pogut revisar, el document d'informació ja inclou una informació sobre protecció de dades que és conforme a l'art. 13 del RGPD.

Pel que fa a la imatge dels treballadors, se'n fa un ús a la targeta d'identificació amb finalitats purament d'identificació dins l'entorn laboral, seguretat i organització de la feina. Per tant, aquest ús ja estaria emparat per la mateixa relació laboral. No obstant, la imatge del treballador es pot fer servir per a finalitats de comunicació. Segons informacions proporcionades a l'àrea de recursos humans, des de l'àrea de comunicació es recolliria el consentiment dels treballadors per a l'ús de la seva imatge amb finalitats de comunicació. No obstant, a l'àrea de comunicació es demana només un consentiment verbal, que no és vàlid, en aplicació del RGPD. És necessari que, si es vol fer servir la imatge dels treballadors per a finalitats de comunicació, es demani el seu consentiment previ, exprés, inequívoc i per escrit, ja que l'ús de la imatge amb finalitats de comunicació no està justificat en la relació laboral i el consentiment ha de ser exprés. En aquest sentit, cal que des de l'àrea de comunicació es faci servir un model d'autorització per a l'ús de la imatge que s'ajusti al RGPD i que informi correctament sobre la finalitat de l'ús de la imatge per a comunicació o difusió en mitjans de comunicació de l'entitat. D'altra banda, sempre és convenient, per una qüestió de minimització en el tractament de les dades i per aplicació de privacitat per defecte i des del disseny, recollir només el consentiment d'aquelles persones, les imatges de les quals s'hagin de fer servir. Una altra cosa és que, tal com hem comentat, un cert ús intern de la imatge amb finalitats d'identificació del personal es pugui dur a terme sense necessitat d'autorització expressa. Recomanem que, en la informació que es proporciona

als treballadors sobre el tractament de les dades s'hi inclogui una menció a l'ús de la seva imatge amb finalitats d'identificació.

Durant el procés d'incorporació d'un nou membre del personal, des de l'àrea de recursos humans comuniquen mitjançant una incidència amb l'aplicació del centre d'atenció a l'usuari (CAU) a l'àrea informàtica que doni d'alta la nova persona amb els accessos informàtics corresponents. Aleshores, des d'informàtica es completa el perfil del nou usuari del directori actiu i se li proporciona accés també als entorns informàtics i recursos necessaris.

Pel que fa a la prevenció de riscos, es du a terme internament, llevat la vigilància de la salut, que està subcontractada amb l'empresa Vitaly. El treballador ha de prestar el seu consentiment per a les revisions de salut, de forma general, tal com podem comprovar amb un model documental aportat com a evidència. No obstant, hi ha diferents tipus de reconeixements mèdics: inicial, periòdics, etc. Hi ha reconeixements que poden ser obligatoris, en alguns casos. D'altra banda, l'entitat compta amb els serveis de Mútua Universal per a la prestació de serveis de mutualitat.

Segons informacions i evidències proporcionades, tal com hem indicat anteriorment en aquest informe, s'han dut a terme diverses accions de formació sota la coordinació de la DPD a través de diferents mitjans. En particular, s'ha implementat una formació online obligatòria sobre protecció de dades que han de cursar tots els membres del personal cada any. No obstant, només un 70% aproximat de la plantilla estaria rebent realment aquesta formació. Seria necessari que es pogués constatar i evidenciar el seguiment i l'aprofitament que fa la plantilla d'aquesta formació a través d'evidències tangibles.

Les baixes dels treballadors es gestionen, com les altes, a través de crear una incidència amb l'aplicació del CAU. Mitjançant aquesta eina es comunica des de l'àrea de persones a l'àrea d'informàtica que doni de baixa els accessos d'una persona (directori actiu, aplicacions assistencials, email, etc.).

No consta que hi hagi un tractament de videovigilància amb finalitat de control laboral dels treballadors.

A banda de les qüestions comentades, no consta que l'entitat faci usos de les dades de les persones treballadores que se situï més enllà de la relació laboral o que impliquin tractaments de dades de categoria especial. Així, per exemple, no consta un ús de dades de geolocalització que es dugui a terme, segons informacions proporcionades.

Les comunicacions amb el personal sempre fan per correu corporatiu o per telèfon. El correu personal dels treballadors només es fa servir per a la gestió dels contractes, però no per a qüestions organitzatives. En definitiva, no es detecten tractaments que puguin tenir la condició de desproporcionats o innecessaris des del punt de vista de la gestió de la relació laboral.

- **Administració**

  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**

  Aquest tractament de dades respon a la finalitat de poder oferir i gestionar 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 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 RAT com a "*Externs*", 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 definitiva, 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
- Docents i 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. Tal com es pot comprovar amb la documentació aportada relativa a la gestió concreta de cada col·lectiu (alumnes, docents, col·laboradors, etc.) 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 docents, es recullen les seves dades mitjançant un formulari que ja inclou la informació de l'art. 13 RGPD.

Els voluntaris poden accedir a l'entitat mitjançant un formulari de la web, presentant-se personalment o enviant un email o fent una trucada telefònica. També poden accedir a través d'actes de captació. En qualsevol cas, el procés d'acollida implica que, després d'una formació de 4 hores, es confirma si la persona vol ser voluntària i aleshores s'emplena una fitxa amb les seves dades al programa "gestió de voluntariat". Al mateix temps que s'emplena la fitxa, es proporciona a la persona voluntària el contracte de voluntariat i un document d'informació sobre protecció de dades i compromís de confidencialitat. Constatem durant els treballs de camp que el procediment és correcte, perquè la fitxa s'emplena quan es proporciona la informació sobre protecció de dades. També comprovem que el formulari de la web per a inscriure's com a voluntari ja inclou un avís legal i autorització per a ús de les dades. En tots els casos, la informació sobre protecció de dades que es proporciona és correcte. Actualment hi ha més de 50 voluntaris a l'entitat.

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. Aquest tractament es fonamenta en un conveni amb l'administració pública, que seria la base jurídica del tractament. Tot i que l'entitat assumeix al RAT que és encarregada del tractament respecte a aquestes dades, caldria revisar si l'administració pública no té una previsió diferent.

Les persones que fan donacions a través de la web proporcionen algunes dades, que constitueixen el tractament denominat al RAT "*Amics de l'Institut Guttmann*". Són dades de 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 el procés de donació ja implica autoritzar l'ús de les dades i accedir a una informació de primera capa sobre el tractament, amb possibilitat d'accedir a la política de privacitat, la qual ja inclou la informació completa de segona capa.

A banda de les qüestions indicades, 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**

Les activitats de comunicació que du a terme l'entitat impliquen tractaments de dades amb finalitats de difusió i publicitat dels serveis oferts i prestats, a més de fomentar col·laboracions de forma directa o indirecta. Aquestes serien les finalitats que justificarien la realització d'aquests tractaments. La base jurídica seria, en alguns casos, l'interès legítim de l'entitat i, en d'altres, el consentiment exprés de la persona interessada.

La comunicació interna es gestiona a través de la intranet corporativa i del correu electrònic corporatiu. Cada quinze dies s'envia cada quinze dies per correu electrònic corporatiu el butlletí "Guttmann al dia" a tots els treballadors i membres del patronat. Cada sis mesos també s'envia als treballadors a casa seva la revista en paper "Fulls".

La comunicació externa es du a terme a través dels següents mitjans:

- Webs corporatives
- Xarxes socials: Facebook, Instagram, X, LinkedIn i YouTube.
- Mailchimp

En general, les webs corporatives fan referència a una política de privacitat que conté una informació exhaustiva sobre el tractament de les dades que és conforme a l'article 13 del RGPD. Els formularis de contacte, de forma ordinària, ja permeten accedir a una informació sobre protecció de dades que l'usuari ha d'acceptar necessàriament.

D'altra banda, tal com hem pogut revisar, a la web corporativa ja hi ha implementat un procés que permet informar sobre l'ús de cookies i acceptar-ne o rebutjar-ne diferents usos, de forma prèvia a la navegació.

La gestió de xarxes socials, a través de les quals l'entitat informa sobre els seus serveis, no implica generalment un tractament de dades. 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) pot implicar 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 a més d'estar degudament legitimada, bé sigui per aplicació del "Trans-Atlantic Data Privacy Network", bé sigui per l'obtenció del consentiment exprés per a la transferència, bé sigui per qualsevol altra causa legitimadora.

Respecte a la newsletter que s'envia per mailchimp, segons informacions proporcionades, els seus destinataris són persones que han assistit a actes organitzats per Guttmann i que han consentit expressament poder rebre informació de l'entitat. Per tant, totes les persones que reben aquest butlletí ja s'haurien inscrit prèviament en un acte concret i haurien sol·licitat expressament rebre informació sobre un tema.

En alguns casos, es pot fer servir la imatge de determinades persones (treballadores o pacients) amb finalitats de comunicació. En el cas dels pacients ja es fa signar un consentiment exprés per a l'ús de la imatge amb finalitats de comunicació. Tal com podem comprovar amb el document "*Autorització Presa d'Imatges i Veu*", el procediment ja permet que els pacients prestin el seu consentiment de forma expressa i inequívoca i siguin informats sobre el tractament de les seves dades. En el cas dels treballadors, segons informacions proporcionades, el seu consentiment s'obté verbalment. Això no és correcte, ja que el consentiment s'ha de recollir de forma expressa. És necessari que sempre que s'hagi d'utilitzar la imatge i/o veu d'un treballador amb finalitats de difusió o comunicació s'hagi obtingut prèviament el seu consentiment exprés i inequívoc.

A banda de les qüestions comentades, no consten altres tractaments que siguin desproporcionats o injustificats des del punt de vista de la comunicació que du a terme l'entitat.

- **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. En realitat, consisteixen en una extensió de la prestació assistencial sòcio-sanitària que realitza l'entitat als seus pacients. La base jurídica seria, per tant, la corresponent a la prestació assistencial a pacients, juntament amb el compliment del contracte que va vinculat a la prestació d'aquests serveis.

Pel que fa a Guttmann Barcelona Life, consisteix en un equipament social format per apartaments adaptats a les necessitats especials dels pacients. 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 els quals hi ha una residència adaptada. En tot cas, l'usuari del servei ha de signar un contracte de servei residencial com a requisit necessari.

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. La finalitat d'aquest servei és 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, 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.

Les càmeres es troben instal·lades als corredors, àrees de trànsit, accessos i perímetre, 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. Només els responsables de l'ISMA de l'entitat poden tenir accés al contingut de les gravacions. Els serveis de vigilància subcontractats poden accedir a les visualitzacions, però no a les gravacions.

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, especialment al costat del control d'entrades, a cadascuna de les plantes i a la sortida dels ascensors. Actualment hi hauria unes 33 càmeres instal·lades.

D'acord amb la informació proporcionada, les dades de videovigilància es conservarien durant un mes i mig. Cal tenir en compte que la Guia de Videovigilància de l'AEPD preveu un termini màxim de conservació de les imatges d'un mes. Per tant, és important no conservar les gravacions durant més temps del necessari i, en cap cas, no superar el mes de termini, llevat, evidentment, que hi hagi una causa justificada per a la conservació).

- **Investigació**

  L'entitat du a terme una activitat de recerca rellevant. De fet, un 25% del personal de l'entitat està involucrat d'alguna manera en projectes de recerca.

  La recerca constitueix generalment una finalitat per ella mateixa i implica un tractament de dades sensibles o de categoria especial. Els projectes de recerca que du a terme l'entitat són dels següents tipus:

  - Projectes col·laboratius en consorci: són projectes que reben finançament extern.
  - Estudis clínics: impulsats per l'entitat, retrospectius o prospectius.
  - Proves clíniques: estudis esponsoritzats per la Farmaindústria.

  Cada mes es reuneix el Comitè de Recerca i Innovació, que avalua i aprova els diferents projectes de recerca que l'entitat vol dur a terme. Tots els projectes han de passar per aquest Comitè. Hi ha projectes en què es demana el consentiment exprés i per escrit dels participants i projectes que es poden dur a terme amb dades pseudonimitzades, sense que calgui demanar aquest consentiment.

  Durant els treballs de camp i amb la documentació aportada com a evidència, comprovem que el model documental que es fa servir per a obtenir el consentiment dels participants ja inclou una informació sobre protecció de dades que és conforme amb l'article 13 del RGPD.

  En general, en els diferents projectes es proporcionen als participants els següents documents:

  - Informació sobre el projecte, que ja inclou la informació sobre protecció de dades, segons article 13 del RGPD.
  - Consentiment de participació en el projecte.
  - Qüestionari de comprovació que el participant ha entès correctament la informació proporcionada.

  És correcte que el consentiment informat de participació es proporcioni de forma separada a la informació sobre el tractament de les dades per a una millor comprensió de la persona participant.

En general, per a la pseudonimització de les dades, l'entitat fa servir la plataforma REDCap. Per tant, d'entrada, ja hi hauria separació tècnica i funcional, perquè només l'investigador principal tindria la clau per a reidentificar, en cas necessari. No obstant, d'acord amb les informacions proporcionades, no hi ha un compromís de no reidentificació que es faci signar al personal investigador. És important en aquest punt tenir en compte els requisits legals de la pseudonimització establerts 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 pseudonimització.
- Compromís de confidencialitat i de no fer cap activitat de reidentificació signat per l'equip investigador.
- Aplicació de mesures per evitar la reidentificació.

Com a possible millora, tenint en compte els requeriments indicats, és important fer signar al personal investigador un compromís de confidencialitat i de no reidentificació de les dades a què tingui accés.

- **GNPT**

Segons les informacions i evidències proporcionades, Guttmann Neuropersonal Trainer (GNPT) és una plataforma online que presta serveis de telemedicina a pacients neurològics. És un producte sanitari que l'entitat comercialitza a hospitals i centres de salut, tot i que podria vendre també directament al consumidor final. La finalitat del tractament és, per tant, la prestació del servei; la base jurídica és el contracte que es fa signar al client, que preveu que l'entitat seria encarregada del tractament de les dades. Tal com podem comprovar amb les evidències documentals proporcionades, el contracte ja inclou correctament la regulació de l'encàrrec del tractament de les dades com a conseqüència del servei prestat, si bé el responsable del tractament que hi consta és realment l'empresa Brain Health Solutions, participada per l'entitat i el Grupo ICA.

Constatem que es va fer una anàlisi de riscos específica sobre aquest tractament, la qual es va documentar. D'aquesta manera, s'haurien tingut en compte riscos i aspectes de licitud, i s'haurien pogut minimitzar de forma positiva.

Segons informacions proporcionades, GNPT disposa d'una certa intel·ligència artificial i planteja propostes terapèutiques als pacients. Tanmateix, sempre hi ha un professional humà que pren realment les decisions. Per tant, no hi hauria realment una situació de risc rellevant, com seria una presa de decisions automatitzada sense intervenció humana.

No consta que hi hagi transferències internacionals de dades en aquest tractament de dades, ja que els servidors de GNPT es troben a Madrid.

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 de dades és conseqüència de l'execució d'un projecte de recerca sobre plasticitat neural, que té algunes especificitats. Les dades dels participants s'obtenen a través d'un formulari de la web https://bbhi.cat/participa, que els participants han d'emplenar. Tal com podem comprovar, per a l'enviament del formulari es demana que s'accepti necessàriament una política de privacitat, però realment no hi ha un enllaç a una política de privacitat que funcioni. Caldria que ja en aquest formulari inicial en què ja es recullen dades personals es proporcionés una informació de primera capa sobre el tractament de les dades i s'hi inclogués un enllaç a una informació sobre protecció de dades completa o de segona capa.

  La base jurídica és el consentiment exprés del participant. El document que ha d'acceptar posteriorment el participant és el document "*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, així com sobre el tractament de les dades.

- **Prevenció del 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 jurídica del tractament és el compliment d'una obligació legal.

  En general es poden fer donacions mitjançant la web de l'entitat a través d'emplenar un formulari i proporcionar les dades bancàries. Tal com podem comprovar, el procés ja preveu que la persona hagi d'autoritzar expressament el tractament de les dades i pugui accedir a una informació sobre protecció de dades que és conforme a l'article 13 del RGPD.

  Segons l'article 32 bis, apartat 4, de la Llei 10/2010 de 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme, és obligatori 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'hauria realitzat informe d'avaluació d'impacte, però caldria que inclogués una distinció més clara entre el risc inherent i el risc residual, que ara no s'hi inclou.

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

- **Empremtes digitals àrea mèdica**

  Segons les informacions proporcionades i el RAT de l'entitat, la dada de l'empremta digital es recull de determinades persones i es fa servir com a mitjà de control d'accés a determinades àrees restringides, com són el quiròfan, el gimnàs, l'àrea mèdica i l'àrea d'infermeria. La finalitat del tractament és garantir la seguretat de determinats accessos. La base jurídica del tractament és la potestat d'organització dels recursos i personal 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. Seria convenient revisar en quines condicions es du a terme la recollida i tractament d'aquesta dada. En particular, seria necessari plantejar una anàlisi de riscos actualitzada i/o avaluació d'impacte sobre el seu tractament i garantir que se n'informa correctament les persones interessades.

- **Medxat / AQUAS i Nova HCE**

  Aquests tractaments de dades responen més a l'ús d'eines informàtiques específiques que no pas a activitats diferenciades, ja que en tot cas les dades tractades corresponen a les activitats de prestació assistencial que du a terme l'entitat. Es constata que aquests tractaments es troben identificats al RAT. També consta que es va fer una anàlisi de riscos sobre aquestes eines en el moment de la seva implementació. Per tant, haurien estat definides i analitzades correctament.

  L'AQUAS i la nova HCE són eines d'accés a les aplicacions gestores de la història clínica del pacient. Pel que fa a l'ús del Medxat, permet fer grups de treball i enviar comunicacions de missatgeria instantània entre professionals. Segons informacions proporcionades, no conté dades de pacients ni es fa servir per a comunicar-se amb els pacients. Es pot fer servir tant al PC com al telèfon mòbil.

  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.

- **Pàrquing / Cafeteria i cuina**

  Aquestes activitats impliquen tractar les dades necessàries per a la gestió d'aquests serveis de 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 pàrquing 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.

- **Estudiants de màster, residents i pràctiques**

  Aquest tractament suposa tractar dades d'estudiants, residents i personal en pràctiques. La base jurídica del tractament és l'execució dels corresponents convenis i el compliment de les obligacions legals aplicables (en aquest sentit, són aplicables les normatives que regulen aquestes modalitats de formació).

  Els processos d'acollida d'aquests col·lectius, tal com hem indicat, s'equiparen als dels altres professionals, segons informacions proporcionades. Per tant, en aquest sentit, ja es proporcionaria una informació sobre el tractament de les dades que seria conforme a l'article 13 del RGPD.

  Tal com hem assenyalat anteriorment, si les dades de les persones en pràctiques s'incorporen en una borsa de treball de l'entitat, caldria indicar que es du a terme aquest tractament en la informació que es proporciona sobre el tractament de les seves dades en el moment de la seva incorporació.

- **Registre assistència pacients**

  Aquest tractament no constava en el RAT analitzat durant l'auditoria anterior.

  Segons informacions i evidències proporcionades, l'entitat fa servir un sistema de reconeixement facial per al registre de l'assistència als pacients de Guttmann Barcelona mitjançant l'aplicació Biostar. Més que no pas un tractament diferenciat, l'ús d'aquesta eina forma part de la prestació assistencial i del tractament de les dades dels pacients. Per tant, la base jurídica aplicable és la mateixa que la corresponent a la prestació assistencial, indicada anteriorment.

  L'ús d'aquest sistema de reconeixement facial és totalment voluntari, si bé se'n recomana i se'n demana l'ús. En qualsevol cas, no es denega mai l'assistència a un pacient que no vulgui o pugui fer servir aquest sistema.

  El sistema registra verifica la identitat del pacient i registra l'hora i la data d'arribada. Atès que la verificació de la identitat del pacient a través d'un sistema de reconeixement facial suposa un tractament de dades de categoria especial, seria necessari dur a terme una avaluació d'impacte i realitzar-ne les actualitzacions necessàries, tal com hem indicat anteriorment.

- **Usuaris de la web Siidon**

  Aquest tractament de dades no apareix identificat com a tal al RAT, però considerem rellevant analitzar-lo en aquest apartat. Caldria valorar la possibilitat d'incloure'l al RAT com a tractament diferenciat o com a part d'un altre tractament, sobretot tenint en compte que no forma part pròpiament de la prestació assistencial.

Segons la web del mateix servei, el SiiDON (Servei d'informació integral de la Discapacitat d'Origen Neurològic) és una iniciativa de l'Institut Guttmann que permet posar a disposició de les persones interessades un contingut informatiu contrastat i útil en relació al món de la discapacitat d'origen neurològic. Amb això, l'entitat pretén facilitar eines i recursos que contribueixin a fer més fàcil l'autonomia funcional, el benestar i la inclusió social de les persones afectades i llurs famílies. Per tant, la finalitat del tractament és la prestació del servei indicat. La base jurídica és la prestació del consentiment a través del procés de registre de la web.

La web disposa d'un procés de registre que ja inclou la necessitat d'autoritzar el tractament de les dades i permet accedir a una política de privacitat, la qual conté una informació exhaustiva sobre els usos de les dades a la web de SiiDON de conformitat amb l'article 13 del RGPD.

- **Canal de denúncies**

Aquest tractament de dades no apareix identificat com a tal al RAT, però caldria considerar la seva inclusió en aquest registre, ja que respon a la implementació d'un canal destinat a facilitar la presentació de denúncies. Per tant, les dades poden ser diferents d'altres tractaments. A través d'aquest canal, podran recollir-se dades de qualsevol tipus de persones amb la finalitat de gestionar-les i assegurar l'anonimat dels denunciants, si és el cas.

Aquest tractament respon al compliment de la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció. Per tant, la base jurídica és el compliment d'una obligació legal.

Tal com podem comprovar en l'apartat corresponent de la web, el procediment definit de presentació de denúncies es gestiona a través d'un formulari de la web. No hi ha, però, una informació sobre el tractament de les dades. Per tant, seria necessari incloure al formulari una informació sobre protecció de dades que sigui conforme a l'article 13 del RGPD.

Els usos del canal de denúncies estan definits en un Reglament que l'entitat posa a disposició de forma pública juntament amb el formulari.

- **Registre de visitants de Guttmann Barcelona**

Aquest tractament de dades no consta al RAT o no sembla estar-hi reflectit d'alguna manera, però caldria tenir-lo en compte i valorar la necessitat que es vegi reflectit al RAT com a tractament diferenciat o com a part d'un altre dels tractaments definits.

Durant els treballs de camp, comprovem que per a l'accés a les instal·lacions de Guttmann Barcelona cal registrar-se com a visitant. En aquest sentit, hi ha un control de visitants, els quals poden ser pacients o persones de qualsevol altre tipus. Per tant, aquest control implica un tractament de dades que pot implicar la recollida de dades de persones no incloses en els altres tractaments ja definits al RAT.

La finalitat del tractament és establir un control de les persones que accedeixen a les instal·lacions de l'entitat i garantir la seguretat dins els seus espais. La base jurídica del tractament pot ser l'interès legítim de l'entitat a l'hora de garantir la seguretat en la prestació dels seus serveis.

En el procés de registre de visitants no consta que es proporcioni una informació sobre el tractament de les dades, que en tot cas hauria de proporcionar-se o ser accessible a les persones que són registrades.

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. En particular, com a àrea de no conformitat rellevant, cal tenir en compte la necessitat de no continuar fent servir un sistema de fitxatge dels treballadors que impliqui fer ús de l'empremta digital, tenint en compte les raons indicades.

5.7. DRETS DE LES PERSONES INTERESSADES

Base legal: Articles 13-23RGPD

Situació actual

L'entitat, tal com hem pogut comprovar amb les evidències i informacions proporcionades, ja té previst un procediment per a l'atenció dels drets sobre protecció de dades. En particular, es constata l'evidència documental de formularis previstos per a l'exercici dels drets de rectificació, supressió, oposició, limitació i portabilitat, els quals són ajustats al RGPD. En aquest sentit, ja estaria 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.

De forma ordinària, és des de les àrees d'admissions que es gestionen ordinàriament les peticions d'accés i rectificació de dades personals. D'altra banda, el DPD atendria l'exercici d'altres drets que s'exercissin a través del seu correu de contacte o altres peticions que revestissin algun tipus de complexitat.

No consta que hi hagi un registre dels drets atesos en temps i forma. En aquests dos anys d'ençà de la darrera auditoria no consten exercicis de drets que hagi atès i registrat el DPD.

Segons informacions proporcionades, el procediment implica per defecte demanar el DNI de les persones interessades per a la seva identificació.

No hi ha constància de requeriments d'entitats de control sobre tutela de drets. No consta tampoc que hi hagi a l'entitat processos de presa de decisions automatitzades sense intervenció humana.

En definitiva, es constaten evidències de l'existència d'un procediment d'atenció de drets sobre protecció de dades, però caldria disposar d'un registre que faci evidència dels drets atesos en temps i forma. També cal evitar que el procediment impliqui demanar per defecte el DNI de les persones, sobretot quan sigui possible identificar les persones per altres mitjans i, per tant, sigui innecessària aquesta petició.

No conformitat

▼	Cal disposar d'un registre dels drets que faci evidència de la seva atenció en temps i forma. Cal evitar demanar per defecte el DNI de les persones que volen exercir els seus drets, sobretot quan sigui possible identificar-les per altres mitjans.

5.8. NOTIFICACIONS DE VIOLACIONS DE SEGURETAT

Base legal: Articles 24 i 33 RGPD

Situació actual

Segons les informacions i evidències proporcionades, l'entitat ja disposa d'un procediment intern de registre d'incidències que es gestiona des de l'àrea de sistemes d'informació. De forma particular, comprovem una mostra de documents de 2024 fan evidència del registre d'incidències. En aquest registre, les incidències sobre protecció de dades porten l'etiqueta "LOPD" i es gestionen amb l'eina GLPi.

El personal coneix l'obligació de comunicar qualsevol incidència a l'àrea de sistemes d'informació. 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.

El protocol de bones pràctiques que es proporciona a tot el personal en el moment d'incorporar-se a l'entitat no conté una instrucció 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.

Segons informacions proporcionades, el juliol de 2022 el DPD va tenir coneixement d'una violació de seguretat que va ser comunicada a l'autoritat de control. No obstant, el procés de notificació va concloure amb l'arxiu de les actuacions. No consta cap altre violació de seguretat d'ençà de la darrera auditoria.

No conformitat

▼	És important 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

	es podria incloure al protocol de bones pràctiques per a un millor coneixement del personal.

5.9. DIFUSIÓ DE FUNCIONS I OBLIGACIONS

Base legal: Articles 24 i 25 RGPD

Situació actual

Segons les evidències i informacions proporcionades, 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.

D'una banda, ja s'han dut accions coordinades pel DPD per a impulsar una difusió dins l'organització de funcions i obligacions sobre protecció de dades i ciberseguretat. En particular, s'ha incorporat una formació específica sobre protecció de dades entre la formació que han de seguir anualment tots els membres del personal. No obstant, segons informacions proporcionades, només un 70% de la plantilla hauria seguit realment aquesta formació.

D'altra banda, el protocol de bones pràctiques que s'ha aportat com a evidència ja conté mesures i instruccions de seguretat que tot el personal està obligat a aplicar, a fi de preservar la confidencialitat i la seguretat en els tractaments de dades. També preveu l'aplicació d'un règim sancionador per al cas d'incompliments. Aquest document es proporcionaria durant la incorporació de noves persones a l'empresa i estaria disponible a la intranet corporativa.

Tota la documentació revisada presenta, en definitiva, un contingut correcte sobre les obligacions del personal en el tractament de les dades i l'aplicació de mesures de seguretat.

Per tot plegat, es garanteix en termes generals un coneixement fonamental sobre mesures de seguretat, funcions i obligacions del personal en matèria de privacitat i seguretat. Per tant, resulta clar que, en termes generals, s'estaria complint la necessitat de difondre obligacions i mesures de seguretat específiques que tot el personal ha de conèixer i aplicar.

Àrees de millora

●	És important garantir i evidenciar que la totalitat del personal ha rebut una formació sobre protecció de dades i ciberseguretat i l'ha compresa. En particular, tal com ha indicat l'AEPD (per exemple, en la recent resolució sobre The Phone House), la formació sobre protecció de dades, per a ser entesa com una mesura organitzativa robusta, cal que tingui els següents requisits: • Obligatòria • Que inclogui un test de superació • No genèrica • Tenir traçabilitat de dates i persones assistents • Ser renovada periòdicament

	Atesa la importància del protocol de bones pràctiques, és important assegurar que es proporciona durant l'acollida d'una nova persona a l'organització i que tot el és conscient que és de compliment obligatori i sap com accedir-hi. Cal valorar també incloure en el protocol de bones pràctiques instruccions o una prohibició sobre fer fotos i gravacions al centre, llevat autorització en contrari.

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

Les polítiques de seguretat definides al document "*Annex 39 Protocol de bones pràctiques amb les dades de caràcter personal 2024_0304*" (protocol de bones pràctiques), que l'entitat proporcionaria al seu personal, ja preveuen mesures de control sobre la informació confidencial a què es pugui tenir accés. En concret s'hi preveuen instruccions sobre com desar i enviar informació confidencial de l'organització, especialment dades de salut. També s'hi preveuen mesures de seguretat i control que tots els treballadors i col·laboradors han de complir, sobretot en relació als accessos segurs a les dades i la conservació diligent de les claus d'accés, però també en relació amb el manteniment d'una política adequada de confidencialitat. S'hi preveuen, per exemple, de forma més concreta, entre d'altres, les següents obligacions:

- Bloquejar l'equip informàtic, en abandonar el lloc de treball, a fi d'evitar accessos no autoritzats.
- Apagar o tancar la sessió en l'equip informàtic, quan s'acabi la feina, encara que sigui temporalment.
- No deixar desatesos ni a la vista documents o papers amb informació confidencial.
- Deixar la taula neta al final de la jornada.
- Fer servir el destructor de paper per als documents de paper que es vulguin eliminar.

D'acord amb les instruccions que l'entitat dona al seu personal, ja es constata que s'han implementat mesures que garanteixen la seguretat i la confidencialitat en els accessos als entorns de tractament de dades.

No detectada

▲	

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, tal com podem comprovar amb la descripció de la xarxa aportat com a evidència (sobretot el document "*Annex 21 Esquema de la xarxa*", entre d'altres), està conformada per diversos ordinadors, servidors i dispositius d'emmagatzematge.

Tota la xarxa informàtica de l'entitat disposa d'un antivirus EDR centralitzat i instal·lat en tots els equips, que l'han de tenir sempre actualitzat. Aquest antivirus avalua el comportament dels equips i servidors per motius de seguretat. D'altra banda, la xarxa està protegida per dos tallafocs perimetrals redundants.

Tots els suports i dispositius estan degudament inventariats, cosa que en permet mantenir el control i l'evolució.

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 la visita presencial i els treballs de camp, l'entitat disposa d'un espai dedicat a Centre de Processament de Dades (CPD) situat al costat de l'àrea de sistemes d'informació.

Aquest espai es troba tancat amb clau, i només les persones autoritzades tenen clau per a accedir-hi. Només algunes persones de l'àrea de sistemes d'informació o de manteniment tenen clau per a accedir-hi.

L'espai dedicat a CPD disposa de les següents mesures de seguretat:

- ✓ Situat al costat de l'àrea de sistemes d'informació (cal passar per aquesta àrea per a poder accedir-hi).
- ✓ Accés autoritzat només a a personal de sistemes d'informació i manteniment.
- ✓ Porta tancada amb clau.
- ✓ Extintor al costat de la porta.
- ✓ 3 sistemes de refrigeració redundants.
- ✓ Càmera de videovigilància.
- ✓ Control de temperatura.
- ✓ Detector de fums.
- ✓ Tots els servidors tenen SAIs, i cada SAI té una font d'alimentació diferent.
- ✓ Generador de contingència.
- ✓ 2 fonts d'alimentació diferents per a cadascun dels equips.
- ✓ 2 Firewalls perimetrals redundants.
- ✓ Antivirus EDR.

En general, les mesures de seguretat observades permeten corroborar l'espai de CPD disposa de condicions de seguretat suficients.

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

Tal com podem comprovar amb el protocol de bones pràctiques, que es proporciona al personal en els processos d'acollida, l'entitat ja ha previst 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 els recursos informàtics proporcionats per l'entitat.

De forma particular, el punt 4.5.1 del protocol de bones pràctiques estableix una prohibició d'emmagatzemar informació en discs durs i tenir fitxers locals, amb aquestes paraules.

"*Tots els documents que hagin de crear o processar les persones treballadores en el desenvolupament de les funcions encomanades dins de l'Institut Guttmann s'han d'emmagatzemar en les unitats de disc habilitades a tal efecte de la xarxa corporatiu o de Sharepoint.*

No està permès emmagatzemar permanentment informació de l'Institut Guttmann en el disc dur dels PCs i equips de treball, excepte en aquelles carpetes que se sincronitzen amb les unitats de xarxa en el núvol."

Per tot plegat, es constata que l'entitat ja ha donat una instrucció expressa sobre la necessitat d'evitar que la informació sobre dades personals es guardi sense aplicar mesures de seguretat i conservació.

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

Segons les informacions proporcionades i el document "*Annex 17 Sistema de seguretat i pla de contingències*", ja hi ha definits diferents procediments de còpia de seguretat que s'apliquen a l'entitat.

El 98% aproximat dels servidors estan virtualitzats, però apliquen igualment els diferents processos de còpia de seguretat definits, que, en termes generals, són els següents:

- A través de Veam Backup, còpies en servidor físic cada 4, 8 o 24 hores, en funció del nivell de criticitat previst per a cadascun dels sistemes.
- Les mateixes còpies definides en el punt anterior es fan també en un servidor exterior de l'empresa Arsys, proveïdor del servei.
- Còpies mensuals en disc extern d'1 Tb de les bases de dades més importants (especialment, la base de dades de la història clínica)

A banda dels processos de còpia de seguretat, també es fan proves de recuperació cada 6 mesos, que garanteix el mateix proveïdor Arsys. Cada dia es rep també un informe sobre la realització de les còpies de seguretat.

D'acord amb els paràmetres descrits, els procediments de còpia de seguretat descrits presenten prou condicions de seguretat com per a permetre recuperar una còpia anterior, en cas necessari.

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

Segons les informacions i evidències proporcionades, ja hi ha diferents perfils d'accés a entorns informatitzats, aplicacions i dades de caràcter personal, d'acord amb les responsabilitats i funcions atribuïdes a cada persona dins l'entitat. Així, per exemple, només els perfils assistencials poden tenir accés a les històries clíniques que es gestionen amb les aplicacions assistencials. A més, l'accés a qualsevol d'aquests entorns sempre pot estar limitat a determinats àmbits, segons les funcions atribuïdes a la persona autoritzada.

Constatem que ja hi ha definits diferents perfils d'accés a les dades, tot i que se'n poden crear de nous, en funció de necessitats. També estan definits els permisos que pot tenir el personal a l'hora de manipular o visualitzar les dades en cadascun dels entorns.

A l'entitat es manté una relació dels usuaris que tenen clau i accessos autoritzats (a través dels controls per empremta digital) per a accedir a espais restringits. D'altra banda, a l'àrea d'informàtica es manté la relació d'usuaris amb accés a dades de caràcter personal i la definició dels seus perfils d'accés autoritzats. Aquesta relació es manté actualitzada, ja que els procediments d'alta i baixa estan degudament definits. Es constata que els processos de baixa del personal ja preveuen la baixa dels accessos autoritzats.

En general, tal com comentàvem al punt anterior, és quan s'incorpora una persona nova a l'entitat que s'apliquen els 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 dels entorns informàtics comença quan a l'àrea de recursos humans comuniquen a l'àrea de sistemes d'informació els accessos que ha de tenir mitjançant l'aplicació "clau de pas". Cada perfil professional va associat a un seguit d'accessos, que són els que s'atorguen des de l'àrea de sistemes d'informació i que seran els necessaris per al compliment de les seves funcions.

Per a l'accés al domini o directori actiu el nom d'usuari és generalment la inicial del nom, el cognom i, en cas necessari, la inicial del cognom. La primera contrasenya es genera aleatòriament, es proporciona en un sobre tancat i és provisional, de manera l'usuari l'ha de canviar necessàriament durant el primer accés. Aquest control d'accés està integrat amb el del correu electrònic, de manera que si es canvia la contrasenya per al directori actiu, també es canvia per al correu electrònic corporatiu. D'altra banda, l'accés per contrasenya presenta les següents característiques de seguretat:

- ✓ Ha de tenir un mínim de 8 caràcters.
- ✓ Composició complexa de la contrasenya, que ha de contenir aquests tipus de caràcters: majúscules, minúscules, caràcters especials i /o dígits.
- ✓ Requereix correu alternatiu per al procés de recuperació de contrasenya.
- ✓ Renovació obligatòria de contrasenya cada 6 mesos.
- ✓ Mesura de bloqueig per inactivitat: 10 minuts.
- ✓ No hi ha mesura implementada de bloqueig per intents d'accés fallits, excepte en el personal de sistemes d'informació.

En el cas de les aplicacions assistencials, estan integrades entre elles i tenen la mateixa contrasenya. El nom d'usuari és una seqüència de dígits i una lletra (per exemple, D12). La primera contrasenya es genera aleatòriament i es proporciona a la persona en un sobre tancat. Com en el cas del directori actiu, aquesta primera contrasenya s'ha de canviar necessàriament durant el primer accés. A més, el sistema de control per contrasenya ha tenir les següents característiques:

- ✓ Mínim de 8 caràcters.
- ✓ Composició complexa de la contrasenya, que ha de contenir aquests tipus de caràcters: majúscules, minúscules, caràcters especials i /o dígits.
- ✓ Renovació obligatòria de contrasenya cada 6 mesos.
- ✓ Mesura de bloqueig per inactivitat: 5 minuts (en alguns casos específics, no aplica per causes justificades; per exemple, al quiròfan).
- ✓ Bloqueig per intents d'accés fallits: després de 3 intents d'accés fallits, es bloqueja l'accés.

Pel que fa al correu electrònic, tal com hem comentat anteriorment, té la contrasenya integrada amb el directori actiu. No obstant, com a garantia de seguretat addicional, l'entorn M2365 incorpora un control per doble factor d'autenticació.

En el cas d'altres entorns i aplicacions que es poden fer servir a l'entitat, es troben dins l'entorn segur del directori actiu i només són accessibles des d'aquest entorn. Per tant, per a accedir a qualsevol d'aquests programes cal haver accedit prèviament al directori actiu.

No detectada

▲	

5.17. ACCESSOS REMOTS

Per a 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, fins i tot amb ordinadors particulars. Segons el procediment descrit, és el responsable corresponent qui ha d'autoritzar l'accés remot.

Segons el tipus d'accés, hi ha dos tipus d'accés remot:

1) Per VPN: Aquest accés es configura mitjançant l'aplicació Open VPN i a través del Firewall i fa servir el nom d'usuari i la contrasenya del directori actiu. Està pensat per a personal que fa servir un portàtil de l'entitat per a la connexió remota. Aquesta és l'opció que s'aplica per defecte per a la connexió remota, i la tenen la major de part del personal amb accés remot autoritzat.

2) Per DW Service: Aquesta connexió remota s'aplica de forma residual a l'entitat i suposa fer servir un sistema d'escriptori remot.

En els accessos remots s'apliquen les mesures de control d'accés i bloqueig per inactivitat que s'apliquen ordinàriament per a l'accés al directori actiu.

Segons les informacions proporcionades, l'entitat té la intenció d'implementar un sistema de doble autenticació per a l'accés a través de VPN.

Per a la sortida exterior de la xarxa, recordem que l'entitat disposa de dos Firewalls sincronitzats que controlen les entrades i sortides d'informació, a banda d'un antivirus EDR centralitzat que es troba instal·lat i actualitzat en tots els equips.

Àrees de millora

●	En aplicació de les previsions de l'entitat i com a millora evident en la seguretat general, convé implementar un sistema de doble autenticació en l'accés remot mitjançant VPN.

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

Segons les informacions proporcionades, tal com podem comprovar amb les evidències aportades, ja hi ha implementat a l'entitat un procediment de revisió de possibles accessos indeguts.

Segons el procediment descrit, un cop al mes el DPD fa servir una aplicació (software SQL) per a veure els accessos de qualsevol història clínica corresponent a un mes. D'aquesta manera, fa una revisió de diversos accessos i, si veiés accessos sospitosos o presumptament injustificats, en donaria trasllat a direcció. Amb això faria un informe mensual sobre possibles accessos indeguts. Entre la documentació aportada com a evidència, comprovem l'existència d'una mostra d'informes mensuals de registres d'accessos a històries clíniques de gener a setembre de 2024.

Tal com podem comprovar, el protocol de bones pràctiques que es proporcionaria al personal ja inclouria una informació sobre l'existència d'una mesura de seguretat que permet controlar el registre d'accessos. D'altra banda, aquest document també estableix un règim de responsabilitat que implica la imposició de sancions per al cas de detectar-se i constatar-se possibles accessos indeguts.

Per tot plegat, hi hauria a l'organització un procediment de revisió d'accessos indeguts que implicaria també l'adopció de mesures correctores, en consonància amb el principi de responsabilitat proactiva que preveu el RGPD per al responsable del tractament.

Àrees de millora

●	Com a possible millora, es podria desenvolupar per escrit aquest procediment en un protocol (amb indicació del número d'històries revisades cada mes, i si s'han triat aleatòriament o per ser de VIPs o de personal de l'entitat, que tenen més risc d'accés indegut) i documentar el resultat de les revisions en informes sobre resultats.

5.19. INVENTARI

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

Situació actual

Segons les informacions i evidències proporcionades, els suports i dispositius que es fan servir a l'entitat per a tractar i conservar dades de caràcter personal estan degudament identificats i inventariats a través del software GLPi, que és un sistema de gestió d'actius informàtics . A més, podem constatar durant els treballs de camp que els suports i dispositius porten etiquetes físiques, que contribueixen a la seva identificació.

Durant els treballs de camp comprovem l'existència i el funcionalment del software GLPi com a eina centralitzada de gestió dels dispositius i suports informàtics, que han de dur instal·lat el software "Iventory" instal·lat. D'aquesta manera, l'entitat disposa d'informació sobre les àrees en què s'ubiquen i els usuaris que accedeixen als equips informàtics.

Tal com hem comentat anteriorment, el protocol de bones pràctiques que es proporciona al personal ja conté instruccions i previsions sobre l'ús de suports i dispositius per a garantir-ne un ús segur i responsable, sota control del responsable del tractament.

En definitiva, l'entitat ja disposa d'un inventari de suports i dispositius degudament actualitzat. D'altra banda, ja es preveu l'actualització i control de l'inventari 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 protocol de bones pràctiques que es proporciona a tot el personal per al seu compliment ja conté una previsió sobre destrucció de documentació en paper 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*".

Aquest punt indicat del protocol fa referència a un protocol específic que ja conté mesures de seguretat destinades a la destrucció segura de suports. Aquest document conté previsions de destrucció segura i confidencial.

Per tot plegat, l'entitat té implementat un protocol i un procediment específic de baixa de suports, segons el qual el cap les baixes s'han de comunicar a l'àrea econòmica i financera i a l'àrea de serveis generals. Aleshores, es procedeix a la destrucció física dels discs durs amb un trepant. Les restes es traslladen a una deixalleria; en aquest procediment hi intervé un proveïdor especialitzat, que emet certificats de destrucció segura.

Pel que fa a la documentació confidencial en paper, podem comprovar durant els treballs de camp que l'entitat disposa de trituradores de paper (a l'àrea d'administració, sobretot) i contenidors de destrucció confidencial (a l'àrea de pacients, especialment).

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

Tal com hem comentat en punts precedents, l'entitat no té suports o dispositius que entrin i surtin habitualment de l'entitat i continguin dades de caràcter personal. Tanmateix, té ja definides un seguit de previsions per al cas que hagi de sortir un dispositiu de les instal·lacions o un correu electrònic que inclogui dades personals.

El protocol de bones pràctiques estableix la prohibició de treure històries clíniques fora del centre sense autorització expressa del responsable del tractament (punt 4.12.5). També estableix que els dispositius que continguin dades de caràcter personal hauran d'aplicar mesures de xifrat o, si no és possible, mesures de compressió amb contrasenya, com ara les corresponents als tipus d'arxiu .zip o .rar (punt 4.7.3). El punt 4.6.6. d'aquest document també estableix de forma molt clara que el personal té prohibit enviar dades confidencials dels pacients als quals tingui accés per motius estrictament professionals per correu electrònic, ja que -segons indica- és un mitjà que no garanteix la confidencialitat. En aquest sentit, només es podrà fer ús del correu electrònic quan les dades s'enviïn xifrades, dissociades i als destinataris autoritzats. També resta prohibit enviar dades confidencials dels pacients a través de smartphones, llevat que s'enviïn amb l'aplicació segura MedXat.

No hi ha actualment un procediment previst i definit per a l'enviament de correus electrònics encriptats.

El software antivirus EDR bloqueja l'ús d'unitats USB o de memòria externa i les deixa en mode lectura. Segons informacions proporcionades, hi hauria la possibilitat d'encriptar aquests dispositius amb Bit Locker, en cas necessari.

Per tot plegat, resulta evident que, en termes generals, l'entitat ha adoptat mesures i ha previst instruccions al personal sobre la sortida de dades fora de l'entitat en condicions de confidencialitat i seguretat.

Àrees de millora

●	Com a millora, caldria definir un procediment d'encriptació per a l'enviament de correus electrònics que continguin dades personals, especialment informació de salut, i caldria que tot el personal tingués clar aquest procediment.

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.

Tota la documentació es troba desada en carpetes, calaixos i armaris, generalment sota clau i amb accés restringit als responsables del seu tractament autoritzat. La documentació que encara es conserva en paper consisteix fonamentalment en consentiments informats i proves complementàries de pacients, històries clíniques antigues (en un arxiu històric passiu), expedients del personal i documentació relativa a procediments que requereixen conservar la documentació, com ara consentiments o certificats. També poden conservar-se residualment alguns documents en relació a determinats programes o procediments que requereixen evidències documentals.

El protocol de bones pràctiques estableix mesures de seguretat que s'han d'aplicar en la custòdia i gestió de documentació en paper que contingui dades de caràcter persona. De forma particular, el punt 4.9.3 del document indicat estableix la següent instrucció:

"*No s'han de deixar desatesos en cap moment papers o documents amb informació confidencial que tinguem sota la nostra custòdia. Quan no s'estiguin utilitzant han de ser arxivats o emmagatzemats sota clau, o destruïts adequadament si el seu ús ja no és necessari*".

Els espais i despatxos en què es guarda la documentació en paper es troben generalment tancats, com és el cas també dels accessos a determinats espais restringits. L'entitat té constància de les persones que tenen una clau o un accés autoritzat.

No es constata durant els treballs d'auditoria 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

Segons 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.

La documentació que es pot arribar a conservar actualment en paper i que contingui dades de categoria especial (dades de salut, per exemple) és generalment complementària o accessòria, ja que gairebé tota la informació necessària es recull, es tracta i es conserva de forma informatitzada a través de les aplicacions assistencials. D'altra banda, no entra ni surt documentació de l'arxiu de forma habitual.

El protocol de bones pràctiques que es proporciona al personal estableix al punt 4.12.2 que caldrà que hi hagi un registre d'entrades i sortides per a l'accés a les històries clíniques en paper: "*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. Així, tal com podem constatar, a l'àrea de pacients hi ha contenidors de destrucció confidencials. En canvi, a les àrees d'administració i gestió de recursos humans es fan servir trituradores de documents. En qualsevol cas, ja hi ha una previsió de destruir tota la documentació que tingui dades de caràcter personal a través d'aquest segurs, en cas necessari. El protocol de bones pràctiques ja instrueix el personal sobre la necessitat de fer servir aquests mitjans.

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

Els arxius en suport paper que té l'entitat ja garanteixen 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 anteriorment en aquest informe, la documentació que es pot guardar encara avui a l'entitat en suport paper i que contingui dades de categoria especial té un caràcter residual. En general, es poden conservar algunes evidències documentals relatives a la prestació del consentiment o la certificació, però la major part de la gestió es du a terme de manera informatitzada.

La documentació en paper que encara es fa servir i es conserva efectivament a l'entitat conforma els arxius o àrees documentals que descrivim a continuació:

Arxiu actiu de pacients: Actualment, des de l'àrea d'admissions només es conserven consentiments informats i algunes proves complementàries de pacients, però ja no hi ha històries clíniques en pacients. La idea general és escanejar-ho tot i pujar-ho la història clínica digitalitzada. En tot cas, la documentació activa dels pacients es troba a la unitat d'hospitalització en calaixos identificats per número de llit. Només hi pot accedir el personal mèdic i d'infermeria. No es troba tancat amb clau, però es troba dins un control d'infermeria, on no hi poden persones alienes al servei.

Arxiu passiu general de l'entitat: Aquest espai d'arxiu es troba a la planta -2, sota custòdia del responsable de l'arxiu, i es troba tancat per una doble porta. El seu accés, per tant, requereix claus de les dues portes. Només personal d'admissions i el responsable de l'arxiu hi tindrien accés autoritzats. Les històries dels pacients hi apareixen ordenades per números d'història i per criteris cronològics. També s'hi guarden aquí expedients antics de recursos humans, documentació passiva d'administració i documentació passiva de recerca (bàsicament, consentiments signats). L'arxiu disposa d'un extintor a l'entrada, un sistema de detecció de fums i una alarma d'incendis.

Recursos humans: Es guarden a l'àrea de direcció de recursos humans expedients de tot el personal dins un armari tancat amb clau, ordenats alfabèticament, sota la custòdia i supervisió del personal d'aquesta àrea. A cada expedient hi ha el CV, la descripció del lloc de treball, títols, la verificació dels títols, entrevistes, contracte laboral, acceptació del codi ètic i del document de protecció de dades, resum de l'acollida, DNI i targeta sanitària, entre d'altres.

Àrea econòmica i financera: En aquesta àrea l'única documentació en paper que encara es conserva és la relativa a prevenció de blanqueig de capitals. Es guarden expedients dins una carpeta, amb noms, còpies del passaports, etc. La informació hi apareix ordenada per ordre cronològic, damunt d'una lleixa i accessible pel personal de l'àrea.

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 processos de reclamació, agraïment, queixa 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 persona responsable de l'àrea d'admissions.

Àrees de millora

●	Cal tenir en compte la necessitat d'aplicar criteris i/o terminis de destrucció de la documentació més antiga i innecessària que ja no caldria continuar conservant.

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 del 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. 5.9. Difusió de funcions i obligacions.
II – BLOC DE MESURES DE SEGURETAT
5.17. Accessos remots. 5.18. Registre d'accessos informàtics. 5.21. Sortida de dades. 5.24. Criteris d'arxiu.
NO CONFORMITAT
I – BLOC GENERAL
5.7. Drets de les persones interessades. 5.8. Notificacions de violacions de seguretat.

A Barcelona, en la data de les signatures electròniques

39334508T PERE RUIZ (R: B58671710)

Firmado digitalmente por 39334508T PERE RUIZ (R: B58671710)
Fecha: 2025.02.07 13:20:59 +01'00'

Pere Ruiz Espinós
- Soci -

Caterina Bartrons Pou

Fecha: 2025.02.07 13:11:49 +01'00'

Caterina Bartrons Pou
- Gerent -