FUNDACIÓ INSTITUT D'INVESTIGACIÓ EN CIÈNCIES DE LA SALUT GERMANS TRIAS I PUJOL (IGTP)

Informe d'Auditoria de protecció de dades de caràcter personal

Protocol número: C-16184

INDEX

1. OBJECTIUS I CONTINGUT

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

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

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

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

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

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

- A falta de concreció per part del responsable o encarregat del tractament de mesures específiques, s'auditarà atenent a l'esquema de mesures de seguretat previst al RLOPD, sempre que sigui compatible i no contrari al RGPD ni a la LOPDiGDD. Les mesures previstes al RLOPD que ja estiguin implantades poden ser útils, però cal analitzar en cada cas si són suficients o és necessari modificar-les.

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

2. METODOLOGIA

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

Tant la planificació com 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, així com també els legals.

Per portar a terme l'execució de l'encàrrec, s'han efectuat les següents actuacions:

- Realització de l'auditoria a través d'entrevistes, qüestionaris, recopilació i supervisió de documents, i anàlisi i revisió de les mesures, controls i procediments de l'entitat.

Elaboració del present Informe d'Auditoria.

El treball d'auditoria s'ha desenvolupat complint els terminis pactats, i s'ha dividit en les fases que s'indiquen a continuació:

- Planificació dels treballs: identificació del/s centre/s de l'entitat i, en el seu cas, encarregat/s de tractament, objecte d'auditoria
- Identificació dels interlocutors
- Recollida de la informació
- Estudi i anàlisi de la informació
- Aclariments
- Lliurament de l'informe provisional
- Correccions i aclariments sobre l'informe provisional
- Lliurament de l'informe definitiu

3. DADES DE L'ENTITAT I TREBALLS EFECTUATS

3.1. DADES IDENTIFICATIVES

3.1.1. Dades Entitat

Entitat	Fundació Institut d'Investigació en Ciències de la Salut Germans Trias i Pujol (IGTP)
CIF	G60805462
Domicili	Carretera de Canyet, s/n 08916 Badalona

3.1.2. Descripció de l'activitat

La Fundació Institut d'Investigació en Ciències de la Salut Germans Trias i Pujol, referida, en endavant, també com IGTP o l'entitat, és un fundació de dret privat que pertany al sector públic sanitari i que presta serveis com a centre de recerca públic ubicat a Badalona (Barcelonès). La majoria dels seus patrons són del sector públic.

La principal missió de l'IGTP i el seu objecte social és fomentar i millorar el coneixement científic per tal de millorar la salut i l'atenció mèdica en general a la nostra societat.

L'IGTP està vinculat a l'Hospital Germans Trias i Pujol (HUGTP), amb qui té un conveni de col·laboració, i forma part del campus biomèdic de Can Ruti. L'IGTP du a terme activitats de recerca per compte de l'Hospital, però essent ell el titular d'aquestes activitats.

L'entitat és un centre CERCA i un membre del Bioclúster recolzat i supervisat pel Govern de Catalunya. També està acreditat com a centre d'excel·lència per l'Institut Carlos III i és per tant, l'encarregat de coordinar la investigació científica del campus, treballant en estreta col·laboració amb els altres centres que s'hi ubiquen.

Les àrees en què l'entitat du a terme les seves activitats de recerca són les següents:

- Ciències de la conducta i abús de substàncies
- Immunologia i inflamació
- Malalties cardiovasculars i respiratòries
- Malalties infeccioses
- Malalties endocrines i del metabolisme, dels ossos i dels ronyons
- Malalties del fetge i de l'aparell digestiu
- Càncer

- Neurociències
- Salut comunitària

3.2. TREBALLS EFECTUATS

S'han revisat i avaluat les següents àrees de l'entitat:

Unitat de de protecció de dades
Gerència
Oficina del DPD de Tic Salut
Àrea d'IT
Centre de processament de dades (CPD)
Unitat de finances
Unitat de gestió de les persones
GCAT (Genomes for life)
Àrea de "fundraising"
Unitat de comunicació
Unitat de projectes
Unitat de laboratori
Unitat polivalent i investigació clínica
Centre de medicina comparativa i bioimatge
Biobanc
Program for predictive and personalized medicine of càncer
Unitat d'innovació
Comitè d'ètica

3.2.1. Dates de realització de l'auditoria

Dates	28 al 29 de setembre de 2023

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	Iris Bargalló	Responsable de protecció de dades
2	Carles Esquerré	Gerent
3	Míriam Méndez	Oficina de TIC Salut i Social, Delegat de Protecció de Dades (DPD)
4	Rubén Cobo	Cap de la unitat d'IT
5	Eva Garcia	Cap de la unitat de finances
6	Paula Amorín	Administrativa del departament de proveïdors

7	Àngels Serra	Administrativa i gestió i facturació de clients i assajos clínics
8	Montserrat González	Responsable de la unitat de gestió de persones
9	Rafael de Cid	Director científic de GCAT
10	Anna Duran	Responsable de mecenatge i d'Amics de Can Ruti
11	Sofía Moresi	Responsable de comunicació del programa Amics de Can Ruti
12	Sílvia Andrade	Responsable de mecenatge i de finances del programa Amics de Can Ruti
13	Tamara Gutiérrez	Responsable de comunicació
14	Òscar Fraile	Cap de l'oficina de projectes
15	Laia Coll	*Lab Manager*
16	David Izquierdo	*Lab Manager* i coordinador de la unitat de *Lab Managing*
17	Magí Farré	Responsable de la unitat polivalent d'investigació clínica (UPIC)
18	Anna Maria Barriocanal	Coordinadora de la unitat polivalent d'investigació clínica (UPIC)
19	Sara Capdevila	Directora tècnica del centre de medicina corporativa i bioimatge (CMCIM)
20	Gemma Monté	Responsable de bioimatge
21	Edurne Pedrosa	Directora científica del Biobanc
22	Miquel Àngel Peinado	Investigador sènior i director del *program for predictive and personalized medicine of cancer*
23	Raül Zurita	Responsable d'innovació
24	Àngels Fortes	Secretaria tècnica del comitè d'etica en la investigació clínica (CEIC)

Relació de la documentació lliurada a l'auditor:

- Resum auditoria 2021.
- Conveni de cooperació amb l'Institut Català de la Salut i la Fundació TIC Salut i Social per a la provisió de serveis de DPD, entre d'altres qüestions.
- Registre Activitats Tractament IGTP v3.
- Escriptura Estatuts adaptats.

- Organigrama definitiu.
- Activitat del centre.
- 20191023 Política de Protecció de Dades v1.
- 20191009 Codi de Conducta de Seguretat de la Informació v1.
- Data Protection (captura de pantalla amb els documents sobre protecció de dades accessibles per al personal a la intranet).
- Welcome Pack (documents que es proporcionen al personal nou):
    - 0. Política prevención empresa.
    - 1. Manual básico PRL.
    - 2. Extracto riesgos puesto administrativo-bio informático.
    - 3. Ficha informativa administrativo-bio informático.
    - 3. Normas de Seguridad en Laboratorio.
    - 4. Extracto medidas de emergencia.
    - 5. Uso de extintores
    - 6. Pautas primeros auxilios
    - 7. Accidentes in itinere.
    - 8. Manipulación manual de cargas.
    - 9. Orden y limpieza.
    - 10. PVD Pantallas.
    - Accés dades Biblioteca de Ciències de la Salut.
    - Acta formación Ley 31 personal administrativo bio informático.
    - Circular 1. Annex calculadora vacances i dies personals.
    - Correu IGTP.
    - Manual portal del empleado.
    - Manual bienvenida IGTP.
    - Modelo datos personales_v5 IGTP_IB.
    - Notificacions altes, baixes i partes Conf x IT.
    - Test curso inicial IGTP personal administrativo bio informático.
    - Vigilancia de la salud.
- Clàusules addicionals (per a incloure en un contracte de treball).
- Formulari d'adscripció a l'IGTP.
- Correu formulari d'adscripció a l'IGTP (model de correu electrònic).
- Model de conveni d'adscripció a l'IGTP.
- Oferta de treball mail resposta (resposta model per correu electrònic).
- Full de dades de protecció de dades (formulari de la unitat de finances).
- PD 001- Procediment de Fuites de Seguretat
- IGTP Registre d'incidències de seguretat.

- Notificació de violació de seguretat CEEISCAT (per part d'Abast Systems Solutions, S.L.).
- Comunicació als afectats 2022-03-21 (per part de l'entitat, sobre violació de seguretat).
- Carta información (per part de l'entitat, informant sobre violació de seguretat).
- 02_01 NVS 16-22 IGTP AR i requeriment.
- 08_01 NVS 16-22 IGTP arxiu-resolució.
- Medidas de seguridad (comunicat tècnic per part d'IT).
- Condiciones de uso de la infraestructura informática de la Institución.
- Copias de Seguridad v2.
- Diagrama catálogo de servicios.
- DR (pla de contingència sobre possible parada tècnica del servei).
- Inventario (de suports i dispositius)
- Política de Seguridad de ficheros.
- Informe Avaluació d'Impacte IGTP_ GCAT-GEMINI.
- AIPD APP-OXA (informe d'avaluació d'impacte).
- Excel contratos 2023 (contractes d'encàrrec de tractament de dades).
- Contractes en què l'entitat és encarregada de tractament de les dades: Ferrer Internacional, S.L. (serveis clínics i de biobanc), Fundació Privada Institut de Recerca de la Sida-La Caixa (serveis de la plataforma REDcap),
- Plec de clàusules administratives particulars
- Contracte d'assaig clínic amb Medpace Clinical Research, LLC. i Institut Català d'Oncologia Badalona.
- Contracte per a un estudi de recerca amb Takeda Development Center Americas, Inc. i Institut Català d'Oncologia Badalona.
- Contracte de transferència de dades per part de ISGlobal.
- Contracte de transferència de dades per part de Katholieke Universiteit Leuven.

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 ha realitzat anteriorment auditories de protecció de dades. Tal com podem comprovar amb l'evidència aportada, el darrer informe d'auditoria porta data de 25/07/2021. D'altra banda, el resultat de l'auditoria es va presentar en un acte públic a tot el personal de l'entitat per part de la responsable de protecció de dades. S'aporta evidència del document de presentació que es va fer servir durant l'acte, al qual també va assistir la direcció. No consta que es documentés l'elevació del resultat a la direcció de l'entitat.

Per tot plegat, podem constatar que ja s'està aplicant una mesura de seguretat de realització d'auditories, el resultat de les quals s'eleva a la direcció de l'entitat, on s'aproven també previsions de millora que tenen compte els resultats obtinguts. No obstant, seria convenient que les auditories es fessin amb una freqüència biennal.

Àrees de millora

●	Caldria elevar el resultat de l'auditoria a la direcció de l'entitat, documentant-ho en una acta per escrit.

5.2. REGISTRE D'ACTIVITATS DEL TRACTAMENT

Base legal: Article 30 RGPD

Situació actual

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

En el cas de l'entitat, els tractaments que du a terme, pel volum i la sensibilitat de les dades tractades, poden implicar un risc per als drets i les llibertats. D'altra banda, també s'hi tracten dades de categoria especial, com ho són per exemple les dades de salut dels pacients. Per tant, en aplicació de les previsions del RGPD, l'entitat està obligada a elaborar i mantenir un RAT.

A data de l'auditoria, l'entitat manifesta i pot evidenciar que ha elaborat un RAT a través del document Excel "*Registre Activitats Tractament IGTP v3*", que aporta com a evidència i que, tal com es pot comprovar, identifica diferents activitats de tractament que l'entitat du a terme com a responsable o com a encarregada del tractament. Com a responsable, du a terme les següents activitats de tractament, segons el RAT:

- Trabajadores
- Trabajadores de Contratas
- Visitantes
- Trabajadores de empresas que alquilan espacios dentro del IGTP
- Miembros del CEIC
- Clientes
- Rescabalaments
- Proveedores
- Amics de Can Ruti
- Comunicación
- Investigadores
- GCAT
- Plataformas: Genòmica, Genómica Translacional, Microscopia, Proteomica
- Biobanc
- Donantes Económicos
- Participantes UPIC
- Pacientes Pruebas Diagnósticas
- Grupos de Investigación
- Neurogenètica
- Videovigilància

Com a encarregada del tractament, s'identifiquen al RAT els següents tractaments:

- Biobanc
- Plataformas: Genòmica, Genomica Translacional, Microscopia, Proteomica

- Participantes UPIC
- Pacientes Pruebas Diagnóstica /CMCiB
- Pacientes Pruebas Neurogenética

El RAT ha estat elaborat com a document Excel i conté una informació completa sobre els diferents tractaments i el tipus de dades tractades. Es comprova que el model de RAT efectivament ja conté correctament emplenats tots els camps previstos per l'article 30 RGPD (finalitats del tractament, categories de dades, terminis o criteris de conservació, destinataris de les dades mesures de seguretat aplicables, etc.), a més d'altres camps addicionals, com ara el que identifica les bases jurídiques corresponents. Com a possible millora, es podria simplificar la gran quantitat de tractaments previstos, agrupant-los per categoria d'interessats i bases jurídiques (per exemple, incloent els participants en projectes de recerca en una mateixa categoria, independentment del tipus de projecte).

Durant els treballs de camp realitzats a la seu de l'entitat no s'han detectat altres activitats de tractament diferents de les que apareixen identificades al RAT. No obstant, caldrà tenir en compte l'existència de nous tractaments que poden anar sorgint, com ara per exemple el derivat de l'existència d'un canal de denúncia, segons es desprèn de l'aplicació 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.

D'altra banda, 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.j de la LOPDGDD.

Àrees de millora

●	Com a possible millora, es podria simplificar la gran quantitat de tractaments previstos, agrupant-los per categoria d'interessats i bases jurídiques (per exemple, incloent els participants en projectes de recerca en una mateixa categoria, independentment del tipus de projecte). També cal tenir en compte l'existència de nous tractaments que poden anar sorgint, com ara per exemple el derivat de l'existència d'un canal de denúncia.

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

Base legal: Articles 24, 25 i 32 RGPD

Situació actual

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

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

L'entitat no té actualment un únic document de seguretat que descrigui de manera integral la seva política de protecció de dades, sinó que disposa de diferents documents que, a tall de protocols o comunicats tècnics, defineixen exhaustivament i de manera integral la política de protecció de dades de l'entitat i les mesures de seguretat que aplica. En són un exemple destacable els documents aportats a aquesta auditoria, que porten els títols:

- Política de Protecció de Dades v1.
- Codi de Conducta de Seguretat de la Informació v1.
- Data Protection (captura de pantalla amb els documents sobre protecció de dades accessibles per al personal a la intranet).
- Welcome Pack (documents que es proporcionen al personal nou)
- Formulari d'adscripció a l'IGTP.
- Medidas de seguridad (comunicat tècnic per part d'IT).
- Condiciones de uso de la infraestructura informática de la Institución.
- Copias de Seguridad v2.
- Diagrama catálogo de servicios.
- DR (pla de contingència sobre possible parada tècnica del servei).
- Política de Seguridad de ficheros.
- Procediment de Fuites de Seguretat.

Tots aquests protocols ja responen a criteris del RPGD i estan degudament actualitzats.

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.
	Quan es produeixin violacions de seguretat, es notificaran a l'autoritat de control en el termini de 72 hores d'ença del

Violacions de seguretat de les dades	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. De manera que 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 documents i protocols 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, tal com podem veure també al RAT de l'entitat, on hi ha un apartat específic de valoració del risc i de la necessitat de dur a terme una avaluació d'impacte.

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.

D'acord amb les informacions i evidències aportades, ja s'han dut a terme accions documentades d'anàlisi del risc i avaluació d'impacte. L'eina que fa servir l'entitat per a la valoració del risc ja permet valorar si hi ha la necessitat de fer o no una avaluació d'impacte en relació a un determinat tractament. D'acord amb la mostra aportada com a evidència, corroborem que els informes d'avaluació d'impacte realitzats en relació al projecte GCAT i a l'aplicació OXA són ajustats al RGPD. Cal tenir en compte que el CEIC de l'entitat té un representant de protecció de dades que, en funció del tipus de projecte que es plantegi, pot requerir també la realització d'una avaluació d'impacte. Els informes els ha dut a terme la responsable de protecció de dades o CPD, i en aquest punt cal dir que això pot plantejar problemes de comptabilitat amb les seves altres funcions de d'assessorament i supervisió. Seria millor, en aquest sentit, que els dugués a terme una altra persona.

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

Àrees de millora

●	Els documents aportats a aquesta auditoria demostren i evidencien que s'han adoptat mesures de seguretat en relació a les activitats de tractament de dades que du a terme l'entitat. Aquestes mesures, tal com estan definides i plantejades, responen en bona mesura a les que ja preveia l'antic RLOPD i resulten adequades. En tot cas, caldrà que aquestes mesures sempre es puguin revisar i actualitzar, tenint en compte les necessitats dels nous tractaments que puguin sorgir i els principis de privacitat per disseny i per defecte. D'altra banda, seria millor que fos una altra persona diferent de la persona responsable de protecció de dades, CPD o DPD, qui dugués a terme els informes d'avaluació d'impacte, a fi d'evitar problemes de compatibilitat amb les altres funcions d'assessorament i supervisió.

5.4. DELEGAT DE PROTECCIÓ DE DADES

Base legal: Article 37 RGPD

D'acord amb el conveni subscrit en data 16/10/2020 amb TIC Salut i Social, aquesta entitat assumeix les funcions del DPD, seguint un model de DPD unificat per a tot el sector públic sanitari de Catalunya. Aquest conveni, que ha estat aportat a aquesta auditoria com a evidència, ja conté les previsions necessàries per a la definició de les tasques pròpies del DPD extern, l'encàrrec de tractament que implica aquesta activitat i la coordinació de tasques amb la pròpia entitat. La Sra. Iris Bargalló assumeix les funcions de Coordinadora de Protecció de Dades (CPD), que també té unes funcions definides dins aquest nou marc de relacions.

Segons el model de DPD del sector públic sanitari, l'Oficina DPD de Tic Salut i Social du a terme les següent funcions per a l'entitat:

- Coordinació de protecció de dades amb tot el sector.
- Proporcionar píndoles informatives.
- Garantir l'eina per a l'elaboració d'AIPD.
- Respondre consultes i facilitar assessorament.
- Mòduls de formació sobre protecció de dades.
- Reunions de coordinació.

S'atribueixen a la CPD, per delegació, algunes de les funcions pròpies del DPD, mentre que es creen també funcions específiques per a aquesta figura, que són:

- Actuar com a enllaç amb el DPD.
- Informar al DPD de les actuacions realitzades.
- Implementar consideracions del DPD.
- Assistir els responsables de l'entitat que intervinguin en protecció de dades.
- Actualitzar el RAT, quan sigui necessari.
- Comunicar al DPD noves activitats de tractament.
- Exercici dels drets dels interessats.
- Incidències i violacions de seguretat.
- Assistir a reunions amb d'altres CPDs.
- Realitzar un informe anual de situació.
- Realitzar tasques d'assessorament intern.

Es confirma, per tot plegat, que a la pràctica qui du a terme el seguiment de la política de protecció de dades a l'entitat és la CPD.

Comprovem que el DPD, a data d'auditoria, ja consta com a registrat a les bases de dades públiques sobre delegats de protecció de dades, accessible a través de les webs de l'AEPD i de l'APDCAT.

Entre la documentació aportada, hi ha l'organigrama de l'entitat. No obstant, la figura del DPD no apareix en aquest organigrama.

El DPD, que consisteix realment en una oficina jurídica especialitzada de TIC Salut i Social, compleix els requisits de formació, experiència i manca de conflicte d'interès.

No consta que hi hagi una freqüència estipulada de reunions de la CPD o DPD amb la direcció de l'entitat amb la finalitat d'exercir les funcions d'informació, sinó que es fa només quan en sorgeix la necessitat.

Sota la coordinació del DPD, s'han realitzat accions de formació al personal, de què s'aporta evidència. En concret, s'han implementat mòduls de formació que preveuen la realització d'exàmens. En aquest sentit, ja s'han realitzat algunes accions de difusió i formació sobre protecció de dades sota la coordinació del DPD.

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 del DPD i la possibilitat de comunicar-s'hi.

Àrees de millora

●	Com a possible millora, caldria incloure la figura del DPD o DPO en l'organigrama de l'entitat. També com a millora, es podria establir una freqüència estipulada de reunions amb la direcció de l'entitat i documentar la informació reportada.

5.5. ENCARREGATS DEL TRACTAMENT I PROVEÏDORS SENSE ACCÉS A DADES

ENCARREGATS DEL TRACTAMENT

Base legal: Article 28 RGPD i disposició transitòria cinquena LOPDGDD

Tal com es pot comprovar, amb la documentació i la informació proporcionades, l'entitat ja du a terme un cert control i seguiment de totes les persones o empreses externes a qui permet un accés autoritzat a les seves dades, i fa signar contractes d'encàrrec de tractament amb totes elles.

Segons la informació facilitada, en general és l'àrea legal la que revisa els diferents contractes amb proveïdors i altres entitats que ha de signar l'entitat i decideix, amb el suport de la responsable de protecció de dades, si cal fer signar també un contracte d'encàrrec de tractament de dades. Tal com podem comprovar amb el document Excel aportat com a evidència, tots els contractes de proveïdors amb accés a dades s'inclourien en un document centralitzat, on es determinaria a qui correspon la seva revisió. No obstant, no consten en aquest document tots els contractes d'encàrrec de tractament de dades que se suposa que ha de tenir l'entitat, com ara el que té amb JDA Expert LegalTax, S.L.P., que presta serveis d'assessorament laboral i contractual. També seria necessari que hi constessin tots els proveïdors tecnològics que tenen accés a les dades.

Es constata que en el plec de clàusules administratives ja s'inclouen previsions sobre el fet que el proveïdor sigui encarregat del tractament de les dades. En aquest sentit, s'ha aportat com a evidència un model de plec que ja conté previsions i clàusules específiques que regulen l'encàrrec de tractament, les quals són correctes.

S'ha aportat a aquesta auditoria com a evidència una relació de contractes signats, però no són d'encàrrec de tractament de dades en què el proveïdor sigui encarregat i l'entitat responsable. En concret, s'han aportat contractes en què l'entitat és encarregada: amb Ferrer Internacional, S.L. (serveis clínics i de biobanc) i amb Fundació Privada Institut de Recerca de la Sida-La Caixa (serveis de la plataforma REDcap). Aquests contractes són correctes i s'ajusten al RGPD.

Tant els contractes d'assaig clínic amb Medpace Clinical Research, LLC. i Institut Català d'Oncologia Badalona com els contractes per a un estudi de recerca amb Takeda Development Center Americas, Inc. i Institut Català d'Oncologia Badalona contenen previsions sobre protecció de dades i confidencialitat, tal com hem pogut comprovar.

Val a dir que d'ençà de 25/5/2018 s'utilitza a l'entitat un model de contracte d'encàrrec de tractaments ajustat als requeriments del RGPD. Els contractes d'encàrrec de tractament de l'entitat anteriors a 25/5/2018 i que continuen vigents han estat actualitzats, tenint en compte la moratòria que finalitzava el 25/5/2022.

Àrees de millora

●	Cal identificar de forma més clara en un document tots els encarregats de tractament de dades que tenen aquesta condició i que han signat un contracte o clàusules d'encàrrec de tractament de dades. Cal revisar que s'han signat contractes d'encàrrec de tractament de dades amb tots els proveïdors que tinguin accés a dades.

	En particular, és important regular els encàrrecs de tractament de dades que pugui haver-hi entre IGTP i l'Hospital Germans Trias i Pujol diferents dels corresponents als projectes de recerca, que sí estan regulats i es fan signar en cada projecte. També es podria establir un conveni marc amb l'Hospital per a la gestió de tota la recerca. És recomanable elaborar i implementar protocol específic que inclogui les previsions de l'entitat sobre 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. Per prevenir aquesta situació de risc i un possible accés indegut, correspondria aplicar un compromís de confidencialitat.

L'entitat no fa signar compromisos de confidencialitat i, per tant, no n'aporta una mostra per a la seva revisió. No obstant, sí que hi ha un procés de contractació que s'ha pogut explicar i documentar i que implica que la unitat legal de l'entitat revisi tots els contractes que s'hagin de signar amb proveïdors amb l'assessorament de la responsable de protecció de dades, a fi de decidir si el contracte implica que hagi d'anar acompanyat d'un contracte d'encàrrec de tractament de dades o qualsevol altre tipus de contracte que inclogui també una clàusula de confidencialitat.

En general, els contractes d'assaig clínic, recerca, transferència de mostres i de dades (anonimitzades) ja inclouen previsions de seguretat i compromisos confidencialitat. A aquest efecte hem revisat els contractes d'assaig clínic amb Medpace Clinical Research, LLC. i Institut Català d'Oncologia Badalona i els contractes per a un estudi de recerca amb Takeda Development Center Americas, Inc. i Institut Català d'Oncologia Badalona.

Àrees de millora

●	Seria convenient implementar el procés de fer signar compromisos de seguretat a proveïdors que puguin tenir un accés a les instal·lacions, sense tenir autoritzat un accés a les dades, identificant específicament aquests proveïdors a l'Excel de contractes.

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

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

Situació actual

S'analitza a continuació, de manera general, la legitimitat de les 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:

- Trabajadores
- Trabajadores de Contratas
- Visitantes
- Trabajadores de empresas que alquilan espacios dentro del IGTP
- Miembros del CEIC
- Clientes
- Rescabalaments
- Proveedores
- Amics de Can Ruti
- Comunicación
- Investigadores
- GCAT
- Plataformas: Genòmica, Genómica Translacional, Microscopia, Proteomica
- Biobanc
- Donantes Económicos
- Participantes UPIC
- Pacientes Pruebas Diagnósticas
- Grupos de Investigación
- Neurogenètica
- Videovigilància

- **Treballadors / Investigadors / Treballadors de contractes / Treballadors d'empreses que lloguen espais dins l'IGTP**

  Actualment l'entitat té una plantilla aproximada de 1.000 treballadors, dels quals 360 són empleats propis i 600 són treballadors acreditats procedents d'altres entitats amb qui l'entitat té un conveni (per exemple, de l'Institut Guttmann, de l'ICO Badalona, de l'Hospital Germans Trias i Pujol o o de l'Institut Josep Carreras, entre d'altres).

  Pel que fa a la gestió dels treballadors i investigadors, el tractament de les seves dades té per finalitat la gestió de la relació laboral i l'organització dels recursos humans a l'entitat. La base jurídica que la permet, en el cas dels treballadors en règim laboral, es fonamenta en la preparació i execució d'un contracte de treball, de conformitat amb l'article 6.1.b) RGPD. En el cas de les persones adscrites (treballadors de contractes), la base jurídica és el conveni d'adscripció que es signa a tres bandes entre l'entitat, la persona i la seva entitat de procedència. En el cas dels treballadors d'empreses que llogues espais dins l'IGTP o col·laboradors, el tractament es basa també en l'execució d'un conveni.

En el cas de la prevenció de riscos i vigilància de la salut, la legitimitat del tractament també deriva del compliment d'una obligació legal, d'acord amb l'article 6.1.c) RGPD.

En general, l'elaboració de les nòmines i la gestió de recursos humans es du a terme de forma externa per part de l'empresa JDA Expert Legaltax, S.L.P., amb qui l'entitat té un contracte d'encàrrec de tractament de dades. Els treballadors poden accedir a les seves nòmines mitjançant una plataforma de l'empresa JDA, identificant-s'hi amb usuari i contrasenya. Determinats elements de la relació laboral, com ara la gestió de permisos i vacances es gestionen a través de la intranet corporativa.

El fitxatge dels treballadors i registre de jornada del personal es realitza a través de l'aplicació CGIT Visual Time, que es pot dur també instal·lada al mòbil. És important tenir en compte que aquesta aplicació inclou una opció de geolocalització, que els treballadors poden tenir activada de manera opcional. No es donen instruccions sobre l'ús d'aquesta opció, però permet recollir i tractar dades sobre ubicació a nivell de zona, no pas de punt. Això pot generar el risc que es recullin i tractin dades de geolocalització de persones sense que estigui justificat ni informat. Per tant, cal que l'entitat doni al seu personal que fa servir aquesta aplicació una instrucció clara de no tenir activada aquesta opció, a menys que se'n valori el seu ús en un futur, després d'avaluar-ne els riscos i l'impacte, si és el cas. El tractament de la dada de la geolocalització no seria, d'entrada, conforme a la normativa, encara que fos involuntària.

Pel que fa a la selecció de personal, la du al terme la mateixa entitat. En general, l'entitat pot posar ofertes a la web pròpia o a col·legis professionals i rebre currículums d'un correu electrònic. Tal com podem comprovar a la web, per a l'enviament de currículums es demana que es faci a través del correu electrònic seleccio@igtp.cat; segons informacions proporcionades, quan es reben CVs per correu electrònic, ja està prevista una resposta. No obstant, tal com podem comprovar amb l'evidència aportada, aquest correu no conté una informació sobre protecció de dades que sigui conforme a l'art. 13 del RGPD. Cal que s'inclogui en aquest model de resposta informatitzada aquesta informació relativa a l'art. 13 del RGPD. No proporcionar la informació de l'article 13 RGPD suposa una àrea de no conformitat amb la normativa.

En general, d'acord amb informacions proporcionades, els currículums es guarden de manera indefinida, llevat que siguin per una acció concreta, cosa que constitueix una àrea de no conformitat amb la normativa. És important definir uns criteris o terminis de conservació de currículums i és necessari incloure aquesta informació en els correus de resposta automatitzada que s'envien a la recepció de currículums.

Durant el procés d'acollida d'un nou membre del personal, se li fa arribar un "*Welcome Pack*", que inclou diferents documents amb instruccions i informacions diverses, però sobretot sobre prevenció de riscos i ús dels recursos de l'entitat, tal com podem comprovar amb les evidències documentals aportades. També se li fa arribar un formulari per a la recollida de dades (el document "*Modelo datos personales v.5*"), el qual, tal com podem comprovar, ja inclou una informació sobre protecció de dades que està ajustada a l'article 13 del RGPD.

Amb el contracte laboral, el treballador també ha de signar unes clàusules addicionals, que ja inclouen també la informació de l'art. 13 del RGPD, unes instruccions de seguretat

i bones pràctiques, un compromís específic de confidencialitat i una autorització expressa per a l'ús de la seva imatge amb finalitats de comunicació i difusió.

Per al compliment de l'art. 13 RGPD, l'entitat ja inclou una informació exhaustiva sobre protecció de dades a la intranet corporativa, accessible per a tot el personal. Aquesta informació, tal com podem comprovar amb una captura de pantalla aportada com a evidència, s'ajusta al RGPD.

Segons informacions proporcionades durant els treballs de camp, les dades dels investigadors que participen en projecten, propis o adscrits, es comuniquen a altres entitats en el context de les sol·licituds de subvencions gestionades des de la unitat de projectes. No consta en els instruments dedicats a proporcionar informació sobre el tractament de les seves dades que s'informi d'aquestes comunicacions. Per tant, com a àrea de millora millora, caldria incloure en aquests textos legals una menció al fet que les seves dades poden comunicar-se a altres entitats amb la finalitat de sol·licitar subvencions per als projectes en què participen.

En el cas del personal adscrit, es demana que emplenin un formulari amb les seves dades a OneDrive, del qual s'aporta evidència. Tal com podem corroborar, el formulari ja conté una informació sobre protecció de dades completa, que alhora remet a l'"*Avís legal i política de privacitat de la web*", que conté una informació encara més exhaustiva sobre protecció de dades.

La prevenció de riscos i la vigilància de la salut les du a terme l'empresa externa MTA. Cal tenir en compte que aquesta entitat, en prestar serveis de vigilància de la salut, es considera responsable del tractament de les dades, si més no pel que fa a aquest servei. D'altra banda, l'entitat compta amb els serveis de la mútua de treball Intercomarcal, que també seria responsable del tractament de les dades.

Pel que fa a l'ús de la imatge del treballador, només es fa servir generalment amb finalitats d'identificació i organització de la feina. No obstant, per al cas que es vulgui fer servir amb una finalitat de divulgació o comunicació de l'activitat investigadora, cal que hagi marcat l'opció del sí i signat les clàusules addicionals del contracte, manifestant així el seu consentiment a l'ús de la imatge amb aquesta finalitat, de manera inequívoca i expressa, tal com preveu el RGPD.

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. En aquest sentit, en termes generals, 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.

- **Visitants / Membres del CEIC**

La finalitat d'aquests tractaments és fonamentalment tenir un control sobre la presència de persones que són de fora de l'entitat, però que accedeixen a les seves instal·lacions. La base jurídica és l'interès legítim de l'entitat i, en cas d'haver-hi un contracte de prestació de serveis, també el manteniment i execució d'aquest contracte.

En general, les dades que es recullen i tracten d'aquests tractaments són les necessàries i imprescindibles per a la finalitat de mantenir un control sobre la seva presència i el motiu

que la justifica. Per tant, en la majoria dels casos, només es recullen i guarden dades sobre la identitat, les dades de contacte i la causa de la seva presència.

Durant els treballs de camp no consta que hi hagi un procés pel qual es proporcioni una informació sobre el tractament de les dades, en el moment de registrar-se com a visitant. Segons informacions proporcionades, hi ha un cartell informatiu que ja proporciona aquesta informació. En qualsevol cas, com a àrea de millora, és convenient assegurar que el cartell permet proporcionar aquesta informació en el registre de visitants, i si no és possible, proporcionar una informació per escrit.

- **Clients / Rescabalaments / Proveïdors.**

Segons les informacions proporcionades, aquests tractaments responen al desenvolupament de relacions comercials amb altres persones físiques o jurídiques i, per tant, a l'establiment de mesures contractuals. La base jurídica del tractament, per tant, és la preparació i execució d'un contracte, bé sigui verbal, bé sigui per escrit.

És a l'àrea de gestió i finances de l'entitat on es du a terme la facturació i comptabilitat de l'entitat.

En relació a facturació de clients, es facturen els assajos clínics i cursos de formació. Pel que fa als assajos clínics, es reflecteixen en les factures emeses per al promotor els codis de participants o pacients, però no contenen mai noms que permetin la identificació de persones. Aquests codis s'assignen en la definició de cada projecte. Només una persona definida en cada projecte té la clau per reidentificar les persones a partir dels codis. Les úniques dades que tenen de participants és de persones a qui s'hagi de fer un pagament (per exemple, per despeses de desplaçament).

En relació a proveïdors, són generalment persones jurídiques i, per tant, la seva gestió no implica el tractament de dades personals. És a l'àrea legal on es gestionen els contractes amb proveïdors, amb assessorament de la responsable de protecció de dades, a fi de decidir si han de signar o no un contracte d'encàrrec de tractament de dades o qualsevol altre tipus de contracte o compromís aplicable en relació al tractament de les dades. Com en el cas anterior, es disposen dades personals de participants en assajos clínics amb l'única finalitat de pagar-los despeses. En qualsevol cas, se'ls ha proporcionat prèviament un full que ja inclou informació sobre protecció de dades, de conformitat amb l'art. 13 del RGPD. Segons informacions proporcionades, la informació sobre protecció de dades la reben tant els participants en estudis, com els ponents que col·laboren en la prestació de serveis de formació, com les persones que presenten justificants de reemborsament de despeses.

Tal com hem comentat, si bé l'entitat no recull ni manté generalment dades personals de proveïdors que siguin persones físiques, no es pot descartar la possibilitat que, en l'establiment de relacions comercials, hi hagi tractaments de dades personals de persones físiques, bé sigui en representació de persones jurídiques o bé en el seu propi nom. Si fos el cas, caldria valorar la necessitat d'implementar processos d'informació sobre protecció de dades.

- **GCAT / Investigadors / Plataformes / Biobanc / Participants UPIC / Pacients proves diagnòstiques / Grups d'investicació / Neurogenètica.**

  La recerca és l'activitat principal de l'IGTP i la que constitueix el tractament de dades més sensibles. La recerca és una finalitat en si mateixa i, tal com consta al RAT de l'entitat, té com a base jurídica, de manera general, en la prestació del consentiment per de la persona interessada, el qual pot ser revocat.

  Segons informacions i evidències aportades, l'entitat du a terme diferents activitats i projectes de recerca molt diferents i clarament identificables i, per això, s'ha optat al RAT per diferenciar-les com a tractaments també diferents, tot i que coincideixen en gran mesura en la finalitat i la base jurídica. Com a regla general, els investigadors principals de cada projecte són els encarregats de sol·licitar els accessos i recursos informàtics necessaris per a cada projecte.

  En general, tots els projectes de recerca i assajos clínics requereixen una avaluació prèvia per part del Comitè d'Ètica d'Investigació Clínica (CEIC) de l'entitat. Aquest comitè, que depèn de l'entitat, té un àmbit territorial i revisa projectes d'altres entitats, com ara de l'Hospital Germans Trias i Pujol, de la Fundació Josep Carreras, de la Fundació de Lluita contra les Infeccions, entre d'altres. Aquest àmbit territorial està aprovat i definit per la Generalitat de Catalunya. D'altra banda, el Comitè té 20 membres aproximadament (segons estableix el decret que el regula) i inclou representants de diferents especialitats, representants de pacients i un responsable de protecció de dades. Tots els membres són nomenats per la Generalitat de Catalunya, segons el procediment previst legalment. El CEIC fa una valoració sobre els aspectes tècnics/metodològics, ètics i de protecció de dades de cada projecte i emet finalment un dictamen, que pot ser favorable, denegatori, o requerir correccions i/o aclariments.

  Segons les informacions proporcionades, en tots els projectes s'apliquen de manera general mesures de pseudonimització o codificació de les dades des del moment que són recollides. Cal tenir en compte que un 90% de la recerca consisteix en assajos clínics promoguts per la indústria i aprovats per l'autoritat reguladora, mentre que el 10% restant són projectes promoguts per l'Hospital o la mateixa entitat que requereixen una aprovació prèvia pel Comitè d'Ètica.

  Cada projecte que es du a terme, tant si és un assaig clínic o un estudi observacional, té el seu propi expedient, que, tal com podem comprovar, inclou un consentiment exprés i una informació sobre el tractament de les dades que és conforme a l'article 13 RGPD. Com a àrea de millora en la transparència d'aquests processos i en la comprensió del pacient, seria necessari tendir a que el consentiment sanitari anés separat del consentiment sobre protecció de dades, com a dos documents diferents. En tractar-se de dos tipus de consentiment diferents, caldria que es gestionessin com a dos documents separats.

  Si bé la majoria de participants dels projectes de recerca són persones que tenen o han tingut problemes de salut, també es duen a terme projectes de recerca amb persones sanes. En alguns casos, està previst que puguin presentar-se persones a un estudi de forma voluntària, i en aquest cas poden signar una autorització per a ser informades d'estudis futurs.

Cada projecte s'avalua de forma específica, i en cada cas és el Comitè d'Ètica qui decideix la base jurídica aplicable. En alguns casos, el consentiment és la base jurídica aplicable. En d'altres casos, s'aplica un model de pseudonimització, tal com es descriuen 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 aplica els següents requeriments:

- Separació tècnica 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.

En el cas del Centre de Medicina Comparativa i Bioimatge, que constitueix una eina important en medicina per a l'avaluació prèvia en models animals de dispositius mèdics (vacunes, medicaments, etc.), poden rebre mostres de pacients, però totes arriben sempre codificades (no contenen dades que permetin identificar persones). Només en el cas d'una col·laboració que desenvolupa en la realització de ressonàncies magnètiques a persones voluntàries, reben noms i codis de persones, i quan venen les persones, se'ls fa signar un consentiment específic per a la ressonància.

En el Programa per a la Medicina Predictiva i Personalitzada del Càncer, que podem analitzar durant els treballs de camp, tota la informació clínica que es comparteix dels pacients es fa sempre de forma codificada. Les mostres sempre van associades a un codi, tant si són del Biobanc propi com si venen de fora.

El GCAT és un estudi de cohorts en què participen prop de 20.000 persones, les quals van signar prestar el seu consentiment entre els anys 2012 i 2014 per a l'explotació i seguiment de les seves dades de forma exhaustiva (també dades de salut) vinculades al seu perfil genètic. En aquest sentit, implica un tractament de dades de categoria especial a gran escala, de manera que s'hi donen les condicions per a la realització obligatòria d'una avaluació d'impacte. Tot i que ja consten com a realitzades avaluacions d'impacte en relació a estudis observacionals que fan ús de les dades del GCAT, caldria valorar si a hores d'ara és necessari legalment fer una avaluació d'impacte sobre el GCAT en conjunt com a projecte i, en cas que es valori que no és necessari, documentar la conclusió per escrit. Segons informacions proporcionades, aquesta valoració ja s'està fent. Això és especialment rellevant en un moment en què es planteja actualitzar el consentiment de tots els participants. Val a dir que s'han A la pràctica, el GECAT també funciona com un banc de dades que permet l'accés a la seva informació pseudonimitzada amb finalitats de recerca.

El Biobanc amb què compta l'entitat té emmagatzemats materials biològics, aplicant criteris d'utilitat pública. Les mostres s'identifiquen a través de codis i es gestionen de manera pseudonimitzada. Cal tenir en compte que el Biobanc ja disposa d'un model de consentiment que té en compte proporcionar una informació sobre protecció de dades de conformitat amb l'article 13 del RGPD.

- **Comunicació / Amics de Can Ruti**

  Aquestes activitats de tractament responen a finalitats de difusió de les pròpies activitats de l'entitat a través de mitjans de comunicació, amb finalitats de difusió de les activitats pròpies i fidelització de persones que realitzen alguna aportació.

  L'activitat de comunicació que du a terme l'entitat implica un tractament de dades, que es faria amb finalitats legítimes de comunicació de l'entitat i difusió dels propis serveis. La base jurídica d'aquests tractaments, tal com consta al RAT, és el consentiment. Com a àrea de millora, seria convenient que s'hi afegís també l'interès legítim, tal com apareix esmentat a l'art. 6.1.f) del RGP, ja que en alguns casos l'entitat podria voler dur a terme una activitat de comunicació amb dades de caràcter personal que podria estar emparada en aquest interès. De fet, ja ho està fent quan envia la newsletter al seu personal per un interès legítim.

  En alguns casos, es pot fer servir la imatge de determinades persones (treballadores o participants en projectes, generalment) amb finalitats de comunicació. En aquests casos, hi ha un procediment que permet recollir un consentiment per a l'ús de la imatge, però no s'aplica correctament, ja que, segons informacions proporcionades, en relació a menors d'edat, de vegades l'autorització es demana oralment als pares. És important que, sempre que es faci servir la imatge de qualsevol persona amb finalitats de comunicació, s'hagi recollit prèviament per escrit el seu consentiment exprés i se li hagi proporcionat, si cal, la informació legal de l'art. 13 RGPD.

  La comunicació interna amb el personal s'articula a través del correu corporatiu i la intranet corporativa.

  La comunicació externa es pot dur a terme a través dels següents mitjans:

  - Web corporativa.
  - Xarxes socials: Instagram i Twitter.
  - Newletter: s'envia cada 3 setmanes a persones que tenen una vinculació contractual amb IGTP.
  - Notes de premsa.

  La gestió de xarxes socials, a través de les quals l'entitat informa sobre els seus serveis, no impliquen 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) implica l'existència de transferències internacionals de dades a països no segurs. Per tant, és important que l'ús d'aquestes xarxes i les transferències que suposen estigui degudament informat a les persones interessades i que se'n reculli, si és el cas, el consentiment exprés per a la transferència. Altrament, s'incorreria en una no conformitat amb la normativa.

  En el cas de les persones voluntàries de l'entitat, tot i que la comunicació amb elles es fa també des de les unitats de comunicació i Fundraising, són recultades per l'Hospital Germans Trias i Pujol. Per tant, en aquest tractament l'Hospital és el responsable i l'entitat actuaria com a encarregada del tractament.

  Un altre aspecte important de la web és el compliment de la normativa vigent en matèria de cookies, que implica la necessitat legal d'informar sobre l'ús de cookies de forma prèvia

a la navegació, oferint la possibilitat d'acceptar o rebutjar aquest ús. Actualment, la web ja respon correctament a aquest plantejament, perquè ja ofereix la possibilitat explícita d'acceptar o regular l'ús de cookies de forma expressa i prèvia a la navegació.

- **Donants econòmics**

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

El programa "Amics de Can Ruti" porta a terme tot el mecenatge del Campus Can Ruti, però és l'entitat qui recull i tracta les dades dels donants. En general, segons informacions proporcionades, no es reben mai donacions econòmiques anònimes superiors a 100 Euros.

Hi ha diferents canals per a convertir-se en donant econòmic, però en general comprovem que a la web una persona pot autoritzar a convertir-se en donant econòmic, ser voluntària o senzillament rebre informació. A la web, la persona ja ha d'acceptar una política de privacitat, la qual conté una informació exhaustiva sobre el tractament de les dades. No obstant, segons informacions proporcionades, hi ha altres canals a través dels quals es poden rebre donacions econòmiques (per exemple, a través d'una gestió telefònica), sense que el procés de donació impliqui que es doni una informació sobre el tractament de les dades. És important que, sempre que els donants siguin persones físiques i, per tant, s'hagin de recollir i tractar les seves dades personals, es proporcioni necessàriament una informació sobre el tractament de les dades ajustada a l'article 13 del RGPD. El fet de no proporcionar una informació de l'article 13 en la recollida de dades personals implica una àrea de no conformitat amb la normativa.

En aplicació de la Llei 7/2021, que ha modificat la Llei 10/2010 de 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme, cal tenir en compte l'obligació de realitzar una avaluació d'impacte sobre el tractament de dades relatiu a prevenció de blanqueig de capitals. Aquesta obligació afecta tots els subjectes obligats per la llei, entre els quals hi ha les associacions i fundacions.

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

- **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.

En total, el sistema de videovigilància de l'entitat consisteix en diferents càmeres instal·lades a l'entrada dels edificis, accessos i corredors.

No consta que es faci servir mai la videovigilància per a finalitats que no siguin el control de la seguretat i els accessos.

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, particularment a les entrades dels dos edificis principals.

D'acord amb la informació proporcionada, les dades de videovigilància es conserven aproximadament durant 15 dies. Només el proveïdor té accés a les gravacions.

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

No conformitat

▼	Vegeu els comentaris anteriors, especialment les parts subratllades, que són les que fan referència de forma més específica a àrees de millora i de no conformitat.

5.7. DRETS DE LES PERSONES INTERESSADES

Base legal: Articles 13-23RGPD

Situació actual

L'entitat ja té un procediment definit per a l'exercici dels drets de les persones interessades, però no consta que estigui documentat. En qualsevol cas, l'entitat té previst 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, en tots els avisos legals (per exemple, a la web) ja s'informa convenientment que el DPD de l'entitat és TIC Salut i Social i s'aporten dades de contacte per a l'exercici dels drets. Segons la distribució de funcions i l'esquema previst pel DPD, seria la CPD la responsable de tramitar i atendre els exercicis de drets.

No consten exercicis formals de drets en els darrers dos anys en què el DPD o CPD hagi hagut de donar resposta. Amb tot, segons informacions proporcionades, es respectarien els terminis previstos legalment per a donar resposta a les sol·licituds d'exercici de drets. No consten peticions que s'hagin atès fora de termini.

Per tot plegat, sembla clar que està previst a l'entitat un procediment actualitzat i ajustat al RGPD per a l'exercici dels drets d'accés, rectificació, oposició, supressió, limitació del tractament i portabilitat de les dades, però no consten evidències que aquest procés estigui documentat o s'estigui aplicant correctament.

Àrees de millora

●	Com a millora, caldria disposar d'un protocol que descrigui el procediment d'exercici de drets i evidències que permetin comprovar casos d'exercici i la seva resposta en temps i forma.

5.8. NOTIFICACIONS DE VIOLACIONS DE SEGURETAT

Base legal: Articles 24 i 33 RGPD

Situació actual

Les informacions i evidències proporcionades aportades per l'entitat, especialment el document "*PD 001- Procediment de Fuites de Seguretat*", confirmen l'existència d'un procediment previst de registre d'incidències i de notificació de violacions de seguretat, que s'ha aplicat correctament. En concret, s'ha aportat un document Excel, on ja apareixen diferents incidències de seguretat documentades en els darrers dos anys i les evidències d'haver-se notificat una violació de seguretat a l'APDCAT, que va acabar arxivada per l'autoritat de control.

D'acord amb el registre Excel aportat, es constata l'existència d'algunes incidències en el tractament de les dades que han estat registrades per l'entitat, que serien un robatori d'una base de dades informada per un proveïdor i una errada en una comunicació.

Tal com hem comentat, també hi ha hagut una violació de seguretat que va ser degudament a l'autoritat de control, en aplicació de l'obligació legal de comunicar violacions de seguretat. Segons la documentació aportada, l'APDCAT va decidir finalment arxivar el procediment.

Segons les evidències i informacions proporcionades, es constata l'evidència d'accions de formació i difusió realitzades tant pel DPD, Tic Salut Social, com per la responsable de protecció de dades, que facilitarien al personal ser conscients de la seva obligació de comunicar incidències o violacions de seguretat sobre dades personals de què tinguin coneixement. A la intranet corporativa el personal també té accés a diferents documents i protocols d'obligat compliment, entre els quals la "Política de Protecció de Dades" ja estableix al seu punt 7 la necessitat que el personal comuniqui obligatòriament i de forma immediata qualsevol incidència de seguretat en el tractament de les dades a la gerència i delegada de protecció de dades.

No detectada

▲	

5.9. DIFUSIÓ DE FUNCIONS I OBLIGACIONS

Base legal: Articles 24 i 25 RGPD

Situació actual

D'acord amb les evidències aportades 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, els documents "*Manual de bienvenida de IT*", "*Codi de Conducta de Seguretat de la Informació*" i "*Política de Protecció de Dades*", que s'han aportat a aquesta auditoria com a evidència, ja contenen mesures i instruccions de seguretat que tot el personal està obligat a aplicar, a fi de fer un ús responsable dels recursos de l'entitat i preservar la confidencialitat i la seguretat en els tractaments de dades. Aquests documents són accessibles per a tot el personal a la intranet corporativa, tal com hem pogut comprovar durant els treballs de camp i en la captura de pantalla aportada també com a evidència.

Segons les informacions i evidències proporcionades, la CPD o responsable de protecció de dades també ha realitzat accions de formació en matèria de protecció de dades destinades al personal. També s'han implementat mòduls formatius sobre protecció de dades amb examen.

És important destacar que, en signar el contracte de treball, està previst que el treballador assumeixi també un compromís de confidencialitat.

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. Tal com hem comentat anteriorment, la "*Política de Protecció de Dades*" ja conté una previsió específica sobre l'obligació que té el personal de notificar al DPD qualsevol incidència relativa a protecció de dades.

Per tot plegat, val a dir que 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.

No detectada

▲	

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

L'entitat ja ha definit una política sobre restricció d'accessos i uns paràmetres de seguretat que aplica a la seva xarxa informàtica.

D'acord amb la informació proporcionada, l'entitat ja ha previst la necessitat que l'accés a les dades i recursos del lloc de treball estigui limitat en funció de les responsabilitats laborals de cadascú. Els entorns informàtics a què pot accedir el personal per al tractament de les dades són fonamentalment el domini, el correu electrònic, la intranet, el SAP (entorn de gestió administrativa) i els programes de gestió de projectes de recerca Fundanet i AniBio.

El correu electrònic està integrat amb el domini, de manera que tindrà el mateix nom d'usuari i la mateixa contrasenya en el control d'accés. D'altra banda, el correu electrònic té implementat un sistema de doble factor d'autenticació, que implica haver de rebre un codi per SMS al telèfon mòbil o fer una trucada per a la seva obtenció. Els altres entorns de gestió (SAP, Fundanet i AniBio) no estan integrats amb el domini i tenen usuaris i contrasenyes diferents.

En general, quan entra un nou membre del personal a l'organització (empleat, adscrit o extern), des de la unitat de gestió de persones envien un formulari emplenat amb les dades de la nova persona per correu electrònic a les següents unitats:

- A l'Àrea d'IT, per a la gestió dels seus recursos informàtics.
- Al Mànager del Laboratori, perquè li facilitin els equips de laboratori.
- Als serveis generals, perquè gestionin la seva targeta d'accés.

Aleshores, des de l'àrea d'informàtica o IT es genera un nom d'usuari i una contrasenya aleatòria provisional per a l'accés al domini, que es proporciona a la nova incorporació. El nom d'usuari consisteix generalment en la inicial del nom i el cognom (i la lletra del segon cognom, si convé). La contrasenya és provisional, i l'usuari l'haurà de canviar necessàriament durant el primer accés de forma obligatòria. La contrasenya és la mateixa per al domini i el correu electrònic.

D'acord amb la informació i evidències proporcionades, la contrasenya per a l'accés al domini i al correu electrònic ha de tenir característiques de robustesa, com ara:

- Ha d'incloure un mínim de 8 caràcters.
- Ha d'incloure caràcters de diferents categories de les següents: minúscules, majúscules, dígits i caràcters especials.
- S'ha de renovar necessàriament cada 180 dies.

- En renovar la contrasenya, no es pot repetir cap de les 10 darreres contrasenyes.

L'accés al domini està protegit per una mesura de bloqueig per inactivitat, segons la qual, l'accés es bloqueja després d'una inactivitat superior a 5 minuts. També s'hi aplica una mesura de bloqueig per intents d'accés erroni, segons la qual l'accés es bloqueja després d'haver introduït 3 contrasenyes errades.

L'accés a internet està protegit per tallafocs i antivirus. D'entrada, hi ha Firewall Fortigate 200F, que actua de forma perimetral i filtra les entrades i sortides d'informació, segons la configuració de seguretat, amb la intenció d'evitar possibles atacs que es produeixin des d'internet. D'altra banda, l'entitat també té instal·lat i actualitzat un Antivirus Strike en cada terminal de treball; aquest antivirus es manté sempre actualitzat en tots els equips informàtics que formen part de l'organització.

Els accessos remots a l'entitat han d'estar autoritzats per la direcció i es vehiculen sobretot a través d'un doble sistema: d'una banda, és possible accedir remotament a través d'un accés VPN amb software Fortinet, el qual permet a determinades persones autoritzades a accedir des de casa seva amb equips propis de l'entitat; en aquest accés, les persones s'han d'identificar en el control d'accés al domini; és un accés configurat a través del Firewall. És l'opció aplicable per defecte a les persones que fan teletreball. La segona opció d'accés remot és a través d'un entorn web, aplicable només a usuaris externs; aquesta opció alternativa permet un accés limitat amb les mateixes credencials d'accés del domini i amb les mateixes condicions de seguretat.

El procediment per a donar de baixa com a usuari autoritzat implica que des de l'àrea de recursos humans s'enviï un correu electrònic a la unitat d'IT. Aleshores, a IT es deshabilita immediatament l'accés al domini de la persona que és baixa, però se li permet que continuï disposant del correu electrònic durant un mes, per motius de gestió.

Les polítiques de seguretat definides al document de funcions i obligacions de seguretat que té l'entitat a la seva disposició ja preveuen mesures de control sobre la informació confidencial a què es pugui tenir accés. En concret s'hi preveuen polítiques de confidencialitat i de pantalla i de taula netes. També s'hi preveu, per exemple, que el personal hagi de mantenir una completa confidencialitat sobre la informació accedida i que hagi de fer servir els recursos informàtics proporcionats per l'entitat de manera responsable.

Com a conseqüència de la implementació del teletreball, l'entitat ja ha desenvolupat unes instruccions específiques sobre teletreball, que ha incorporat al "*Codi de Conducta de Seguretat de la Informació*", tal com podem comprovar amb l'evidència documental.

Per a l'accés físic a les instal·lacions i als espais de tractament de dades, està previst que només el personal autoritzat pugui accedir als llocs on es troben instal·lats els equips físics que donen suport als sistemes d'informació. En general, a banda dels accessos per clau mecànica, hi ha accessos restringits que requereixen l'ús d'una targeta.

Pel que fa a la documentació en paper, es troba tota desada en despatxos tancats amb clau, dins armaris, ordenada per criteris cronològics o alfabètics. Es constata, per tant, que tots els espais, magatzems, despatxos i àrees de l'entitat que contenen o guarden documentació amb dades de caràcter personal disposen de sistemes de tancament, de manera que la informació es troba

conservada de forma segura i fora de l'abast d'usuaris no autoritzats. El personal coneix la seva obligació de tancar amb clau les sales i despatxos que continguin informació confidencial, quan ja no es fan servir o quan acaba la jornada laboral.

Finalment, les sales dedicades a servidors es troben tancades quan no es fan servir, i només són accessibles per personal autoritzat.

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 està conformada per diferents ordinadors, servidors i dispositius d'emmagatzematge. L'entitat també disposa d'un espai dedicat a Centre de Processament de Dades, que només és accessible a través d'una doble porta i de passar un control d'accés per targeta. Només les persones autoritzades (personal d'IT) hi tenen accés, i tots els accessos queden registrats.

Tota la xarxa informàtica de l'entitat, a banda de disposar d'un Firewall Fortigate 200F perimetral, que controla les entrades i sortides d'informació des d'internet, també disposa d'un antivirus Strike instal·lat a tots els terminals de treball.

L'entitat disposa d'un procediment per a l'autorització d'accessos remots als seus sistemes a través de VPN mitjançant el software Fortinet. En el cas de l'accés remot per VPN al correu electrònic, es requereix una doble autenticació. També hi ha un accés alternatiu remot a través de la web. En tot cas, l'entitat disposa d'un control i registre sobre els usuaris autoritzats. L'accés remot està protegit per un control d'accés segur que ofereix garanties de seguretat al mateix nivell que l'accés dins l'entitat. Per tant, ja s'hi apliquen mesures de control i actualització suficients.

Tots els suports i dispositius estan inventariats, tal com podem comprovar amb un document Excel aportat com a evidència.

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, l'entitat disposa d'espais que contenen que el Centre de Processament de Dades (CPD) en els edificis de Mar i Muntanya.

Només el personal autoritzat (segons informacions proporcionades, personal de la unitat d'IT) disposa d'accés als espais habilitats com a CPD a través de targeta. Les instal·lacions estan proveïdes de diferents mesures de seguretat:

- Doble control d'accés per targeta.
- Registre de tots els accessos.
- Detector de focs.
- Doble sistema redundant de refrigeració.
- Sistema de control de temperatura i alarma per email.
- SAI, que permetria alimentar el servidor durant 15 minuts i tancar-lo ordenadament, en cas d'interrupció sobtada del corrent elèctric.
- Doble connexió al corrent elèctric i al SAI.
- Firewall perimetral, que permet controlar entrades i sortides d'informació al servidor
- Extintors fora de la sala del servidor.

En general, les mesures de seguretat observades permeten corroborar que el Centre de Processament de Dades 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 "*Codi de Conducta de Seguretat de la Informació*", que conté instruccions sobre seguretat en el tractament de les dades i que és accessible per a tot el personal a través de la intranet, l'entitat ja ha previst instruccions específiques sobre com emmagatzemar o tractar dades de caràcter personal de manera responsable en relació als equips i dispositius.

De forma particular, el punt 2.3.2 del document indicat estableix que "*el personal de l'IGTP i el personal adscrit només podrà descarregar dades mèdiques no anònimes dins l'entorn segur de les instal·lacions del L'IGTP. No es permet la descàrrega o la transferència de dades que continguin identificadors semi anònims en ordinadors personals o domèstics. Si les dades es baixen amb finalitats de còpia de seguretat, s'ha de fer directament en un sistema reconegut com a segur (bloquejat, xifrat, etc.)*".

L'apartat 4 del document indicat també conté previsions sobre l'ús responsable de dispositius mòbils, equips o suports informàtics que continguin dades. Aquests equips, si contenen dades que permetin la identificació de les persones, es podran treure fora de les instal·lacions de l'entitat només si compten amb l'autorització del responsable del departament corresponent. També es contenen en els punts d'aquest apartat previsions sobre les mesures de seguretat aplicable en la protecció de la informació i el seu emmagatzematge segur.

D'altra banda, altres punts i apartats del document esmentat també contenen instruccions sobre l'ús, transferència i conservació de dades en relació al teletreball o a l'ús de dispositius propis, sempre aplicant criteris de confidencialitat i restricció de l'accés.

Per tot plegat, la regla general és treballar de manera responsable amb els recursos i programes proporcionats per l'empresa, que permeten desar tota la informació al servidor, i alhora abstenir-se de fer servir altres dispositius, a menys que es disposi d'una autorització expressa. En tot cas, si cal desar dades de caràcter personal en dispositius de forma autoritzada, s'haurà de fer aplicant mesures de pseudonimització i tenint en compte que caldrà esborrar la informació en acabat, un cop ja no sigui necessària.

No detectada

▲	

5.14. CÒPIES DE SEGURETAT

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

Situació actual

D'acord amb el document "*Copias de Seguridad-V2*" i les informacions proporcionades, l'entitat té implementats diversos procediments de realització de còpies de seguretat, que han estat definits i profusament descrits en el document indicat. De forma resumida, els processos descrits són els següents.

- Còpia *in situ* – Còpia diària, setmanal i mensual amb diferents terminis previstos de retenció. Es col·loquen en suports físics diferenciats i separats, en funció dels seus terminis de retenció.

- Còpia mensual al núvol d'Amazon amb una retenció de 6 mesos.

- Còpia en cinta – Aquest procés encara està pendent de definir-se de manera definida, però la previsió és que es faci amb una freqüència setmanal.

D'altra banda, ja es fan revisions i proves de restauració cada 6 mesos sobre els diferents els procediments de còpia, segons una selecció aleatòria, que resten documentades.

D'acord amb els paràmetres descrits, els procediments previstos de còpia de seguretat ofereixen prou condicions de seguretat com per 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, segons les funcions que tingui cadascú i el seu perfil (empleat, adscrit o extern), tindrà accés restringit a determinats entorns informàtics i carpetes. Els entorns i recursos informàtics rellevants a què pot tenir accés una persona són el domini, el correu electrònic, el SAP (gestió administrativa), el Fundanet (gestió de recerca) i l'AniBio (gestió de recerca).

També estan definits els permisos que pot tenir el personal l'hora de manipular o visualitzar les dades en cadascun dels entorns.

A l'entitat es manté una relació dels usuaris que tenen targeta d'accés als espais restringits.

A l'àrea d'IT 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 hi ha procediments d'alta, modificació i baixa d'usuaris que permeten una comunicació entre les unitats d'IT i gestió de persones.

En general, tal com comentàvem anteriorment, 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, quan entra un nou membre del personal a l'organització (empleat, adscrit o extern), des de la unitat de gestió de persones envien un formulari emplenat amb les dades de la nova persona per correu electrònic a les següents unitats:

- A l'Àrea d'IT, per a la gestió dels seus recursos informàtics.
- Al Mànager del Laboratori, perquè li facilitin els equips de laboratori.
- Als serveis generals, perquè gestionin la seva targeta d'accés.

Aleshores, des de la unitat IT generen un nom d'usuari i una contrasenya aleatòria provisional per a l'accés al domini, que es proporciona a la nova incorporació. El nom d'usuari consisteix generalment en la inicial del nom i el cognom (i la lletra del segon cognom, si convé). La contrasenya és provisional, i l'usuari l'haurà de canviar necessàriament durant el primer accés de forma obligatòria. La contrasenya del domini i el correu electrònic estan integrades.

Segons la informació proporcionada, la contrasenya per a l'accés al domini i al correu electrònic ha de complir requeriments de complexitat:

- Ha d'incloure un mínim de 8 caràcters.
- Ha d'incloure caràcters de diferents categories de les següents: minúscules, majúscules, dígits i caràcters especials.
- S'ha de renovar necessàriament cada 180 dies.
- En renovar la contrasenya, no es pot repetir cap de les 10 darreres contrasenyes.

S'apliquen també en l'accés al domini mesures de bloqueig per inactivitat i intents d'accés fallits. Segons la mesura de bloqueig per inactivitat, l'accés es bloqueja després de 5 minuts sense activitat. En aplicació de la mesura de bloqueig per intents d'accés erroni, l'accés es bloqueja després que s'hagin introduït 3 contrasenyes equivocades.

En el cas del correu electrònic, el seu accés inclou un doble factor d'autenticació, que implica haver de rebre un codi d'accés addicional per SMS, o alternativament fer una trucada per a l'obtenció del codi.

L'accés a internet està protegit per tallafocs i antivirus. D'una banda, el Firewall Fortigate 200F actua de forma perimetral i filtra les entrades i sortides d'informació, segons la configuració de

seguretat, amb la intenció d'evitar possibles atacs que es produeixin des d'internet. D'altra banda, l'entitat també té instal·lat i actualitzat l'Antivirus Strike en cada terminal de treball, que es va actualitzant i que està controlat de forma centralitzada.

Hi ha altres aplicacions que es fan servir a l'entitat per a la gestió administrativa i de projectes de recerca, com ara els entorns SAP, Fundanet i AniBio, però el seu accés no està restringit per la necessitat de disposar de contrasenyes complexes o robustes, si bé el seu accés està subeditat a la necessitat d'accedir prèviament a l'entorn de domini.

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. Des de la direcció de l'entitat és d'on es decideix que un usuari pugui accedir remotament.

A l'entitat estan implementats dos tipus d'accés remots:

És l'opció aplicable per defecte a les persones que fan teletreball. La segona opció d'accés remot és a través d'un entorn web, aplicable només a usuaris externs; aquesta opció alternativa permet un accés limitat amb les mateixes credencials d'accés del domini i amb les mateixes condicions de seguretat.

1- Accés a través de VPN per mitjà del software Fortinet. Aquest és l'accés per defecte aplicat a l'entitat, el qual permet que determinades persones puguin fer teletreball. El control d'accés és el mateix que el del domini. El teletreball només es pot fer a través d'equips propis de l'entitat o administrats per ella.

2- Accés alternatiu via web a l'entorn de domini. Està pensat per a usuaris externs, i implica accedir al domini de forma limitada mitjançant credencials de domini

Per a la sortida exterior de la xarxa, recordem que l'entitat disposa d'un Firewall Fortigate 200F, que controla les entrades i sortides d'informació. També té instal·lat i actualitzat un Antivirus Strike a tots els equips.

Amb la difusió del teletreball, ja s'han dut a terme acciones destinades a prevenir riscs. En concret, s'han inclòs al "*Codi de Conducta de Seguretat de la Informació*" previsions de seguretat sobre aquesta modalitat de treball i sobre l'accés remot als entorns de tractament de dades.

No detectada

▲	

5.18. REGISTRE D'ACCESSOS INFORMÀTICS

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

Situació actual

Segons les informacions i documentació proporcionades, l'entitat disposa d'eines que li permeten dur a terme el registre i control dels accessos informàtics. El programa Faronix, per exemple, permet dur a terme un seguiment i control d'accessos als equips i dispositius informàtics.

Encara que l'entitat acrediti disposar d'eines i recursos adequats per a controlar i monitoritzar els accessos, no realitza revisions periòdiques dels intents d'accés i dels accessos a la informació més sensible. En aquest sentit, no està previst un procediment de realització de revisions periòdiques.

Per tot plegat, l'entitat podria obtenir la informació rellevant sobre els accessos, però aquesta actuació es duria a terme de forma reactiva.

En qualsevol cas, resulta evident que l'entitat du a terme tractaments de dades a gran escala de categoria especial que requereixen l'adopció de mesures de control significatives, com ara el registre i revisió sistemàtica dels accessos, en prevenció de possibles accessos indeguts per part del personal autoritzat.

Àrees de millora

●	Com a millora, es pot implementar un procediment de revisió de possibles accessos indeguts, que caldria definir i documentar. Aquest procediment podria incloure revisions de documentació aleatòria amb informació sensible sota la supervisió de la CPD.

5.19. INVENTARI

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

Situació actual

Segons les informacions proporcionades, els suports i dispositius que es fan servir a l'entitat per a tractar i conservar dades de caràcter personal estan degudament etiquetats, identificats i inventariats.

Tal com podem comprovar durant els treballs de camp, els suports i dispositius duen etiquetes físiques que els permeten identificar. Cada equip informàtic de l'entitat o mòbil d'empresa està associat a un lloc de treball, cosa que permet identificar, en la majoria dels casos, la persona a qui correspon. No obstant, hi ha alguns ordinadors que són compartits entre diversos usuaris.

Comprovem el document "*Inventario*" en format Excel com a evidència, que conté la relació actualitzada d'equips, suports i dispositius associats a usuaris o llocs de treball.

A l'entitat es fa servir també el programa Faronix per a la gestió de l'inventari de suports i dispositius i controlar actualitzacions.

En definitiva, resulta clar que tots els equips i dispositius que es fan servir a l'empresa per al tractament de les dades ja estan correctament inventariats, i que l'inventari es manté degudament actualitzat.

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

Pel que fa a la documentació ordinària de paper que contingui dades de caràcter personal, constatem que l'entitat disposa de màquines trituradores. Així, per exemple, durant els treballs de camp constatem que hi ha una màquina trituradora a la unitat de gestió de persones.

L'entitat també disposa de contenidors de destrucció segura, que són buidats regularment, de manera que la informació que contenen és destruïda de forma segura i certificada per empreses especialitzades.

L'entitat no genera volums rellevants de documentació, més enllà de la documentació necessària per a la gestió dels contractes laborals, determinada documentació administrativa i de facturació o altra documentació relativa a projectes de recerca que requereixen la conservació dels suports.

El "*Codi de Conducta de Seguretat de la Informació*" ja conté una previsió específica sobre la necessitat d'eliminar documentació en paper que ja no sigui necessària de forma segura al seu punt 2.3.3: "*Els documents que continguin informació confidencial es destruiran mitjançant una trituradora de documents o un altre servei de destrucció segura*".

Pel que fa la destrucció de suports i dispositius que continguin dades de caràcter personal de forma segura, d'acord amb les informacions proporcionades, s'apliquen procediments de destrucció física. En general, els discs durs són retirats i proporcionats a una empresa de destrucció segura, que emet certificats de la seva destrucció, cosa que permet registrar la sortida i destrucció dels suports.

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

En general a l'entitat no consta l'existència de transmissions d'informació de forma sistemàtica que contingui dades sensibles o de categoria especial.

Segons informacions proporcionades, no hi ha un procediment específicament definit d'encriptació, que s'estigui aplicant. No obstant, per a la compartició de documentació amb informació sensible fa servir habitualment a tota l'entitat l'entorn OneDrive, que ja requereix contrasenya i suposa l'ús d'un núvol institucional. Segons informacions proporcionades, aquest entorn es fa servir, per exemple, per a enviar-se contractes i nòmines amb la gestoria.

Malgrat no haver-hi un procediment específicament previst, el punt 2.3.1 del "*Codi de Conducta de Seguretat de la Informació*" instrueix el personal en la necessitat de protegir els fitxers que s'hagin d'enviar o compartir amb una contrasenya, quan continguin dades personals o informació confidencial.

Cal tenir en compte que el correu electrònic de l'entitat, per al seu accés, ja requereix per defecte un doble procediment d'autenticació.

Durant els treballs de camp, segons les informacions proporcionades, ja s'estan aplicant procediments d'encriptació en diferents àrees. Així, per exemple, els Excels i els arxius que es fan servir a la unitat de Fundraising per a la gestió de les dades estarien protegits per contrasenya.

No detectada

▲	

5.22. EMMAGATZEMATGE EN SUPORT PAPER

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

Situació actual

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

En general, tota la documentació es troba desada en 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 els expedients dels diferents estudis de recerca i els expedients de la unitat de gestió de persones, si bé hi pot haver alguna altra documentació corresponent a diferents àrees que hagi de ser conservada com a evidència.

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

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

No detectada

▲	

5.23 REGISTRE D'ACCESSOS DOCUMENTAL

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

Situació actual

Segons informacions i evidències proporcionades, la documentació en suport paper que es fa servir a l'entitat es troba generalment desada als seus corresponents armaris, situats en despatxos o sales específiques d'arxiu, que es troben sempre tancats, quan no es fan servir.

En general, la tendència és a conservar cada cop menys documentació en paper, i a escanejar la documentació en paper que pugui arribar a l'entitat d'alguna manera i hagi de conservar-se. Tanmateix, hi ha encara alguns arxius actius en diferents àrees de treball. En aquestes àrees, les poques persones que tenen accés autoritzat a la documentació són els responsables i usuaris autoritzats de les pròpies àrees.

L'entitat disposa d'un espai destinat a arxiu passiu en un edifici annex que es troba sota la responsabilitat de la unitat de serveis generals.

No consta que els procediments d'accés a la documentació en paper que s'apliquen a l'entitat hagin estat definits documentalment. Per a l'accés a documentació antiga desada a l'arxiu passiu, cal demanar-ho als responsables de serveis generals a través d'un procediment ja previst que permet registrar les sol·licituds. En general, la documentació relativa a estudis observacionals s'ha de conservar durant 15 anys, mentre que la documentació relativa a assajos clínics requereix una conservació mínima de 25 anys. De forma habitual, només el personal destinat a l'àrea d'arxiu hi té accés autoritzat, a més dels responsables de seguretat de i manteniment. Aquest espai es troba sempre tancat amb clau. L'accés a la documentació ja implica, per tot plegat, un control i registre de les persones que hi tenen accés.

En general, l'entitat ja disposa de mitjans i recursos per a la destrucció segura de documentació confidencial, com ara màquines trituradores i contenidors per a la destrucció confidencial.

No detectada

▲	

5.24. CRITERIS D'ARXIU

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

Situació actual

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

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 guarda documentació del personal per a la gestió de la relació laboral en els seus corresponents expedients, i es poden conservar algunes evidències documentals relatives a la prestació del consentiment, però la major part de la gestió es du a terme de manera informatitzada. En relació als estudis de recerca, es conserva també documentació, sobretot a l'arxiu passiu, on es guarden expedients anteriors a la difusió de les eines informàtiques.

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

Arxiu actiu de gestió de persones: Es conserven expedients físics del personal, dins un armari tancat amb clau, ordenats per números, sota la custòdia de la responsable de la unitat. La documentació es guarda generalment pseudonimitzat, i no només per a la gestió de la relació laboral, sinó també per a servir d'evidència en l'acreditació dels projectes. Els expedients físics contenen: contracte, autorització de dades i quitança, entre d'altres documents. D'altra banda, quan un treballador és baixa definitiva, el seu expedient és traslladat a l'arxiu passiu, on es continuarà conservant codificat de manera indefinida, per tal de continuar servint com a evidència del personal involucrat en els diferents projectes de recerca. Pel que fa als procediments de selecció de personal, val a dir que els currículums es guarden de manera indefinida també sota els mateixos criteris descrits.

Arxiu de la unitat de finances: Es conserven en aquesta unitat factures de servei, de compra i de rescabalament (reemborsaments de despeses), sota responsabilitat del cap de la unitat. Aquests documents es guarden dins armaris tancats amb clau, ordenats per número i per data de factura. Solen contenir molt poques dades de caràcter personals, excepte en els rescabalaments, que identifiquen la persona que els rep.

Arxiu de projectes de recerca: En aquesta àrea es conserva la documentació i els expedients de la unitat de projectes, sota la seva custòdia i dins un armari que es pot tancar amb clau. Els expedients hi apareixen ordenats per convocatòria i any. Són expedients no actius, ja que ara com ara ja no es genera documentació en paper per part de la unitat de projectes.

Arxius d'assajos clínics i recerca promoguda per l'Hospital o l'entitat: En aquesta àrea es conserven expedients dels diferents projectes, que corresponen realment als diferents investigadors, més que no pas a la unitat polivalent i d'investigació clínica. Els documents hi apareixen registrats per criteris cronològics, només accessibles per als investigadors i els membres de l'esmentada unitat, que també en són els custodis.

Arxiu en paper del Centre de Medicina Comparativa i Bioimatge: En aquest centre només es guarden dins un armari tancat amb clau els consentiments signats per les persones que se sotmeten a ressonàncies o altres estudis, mentre duren aquests estudis. Els consentiments estan classificats per número d'estudi.

Arxiu passiu general: Situat en un espai annex a l'hospital i dotat de sistemes de tancament, només és accessible pel personal responsable de l'arxiu, manteniment i seguretat. Aquí s'hi mantenen desats els assajos clínics i els estudis observacionals antics, que tenen períodes definits de conservació mínima de 25 i 15 anys respectivament. També s'hi conserven expedients laborals antics, a més d'altra documentació financera i administrativa antiga, com ara contractes amb proveïdors i altres entitats. Els responsables de l'arxiu passiu poden atendre les peticions d'accés i proporcionar la documentació. Ja hi ha previstos procediments d'accés a la documentació antiga, que permeten registrar les sol·licituds.

Tal com podem comprovar, tota la documentació es troba correctament desada, ordenada i tancada amb clau dins armaris. Només les persones responsables de cada àrea disposen de clau de cadascun dels armaris.

Àrees de millora

●	Cal evitar conservar de forma indefinida documentació en paper i dur a terme accions de destrucció de documentació antiga, sobretot si és documentació innecessària per a la finalitat que en va motivar la recollida i hagin prescrit els terminis de conservació obligada, si són aplicables. Així, per exemple, a la unitat de gestió de persones de treballadors es conserven currículums de manera indefinida. En aquest cas concret, s'hi podria establir un termini d'un any. En definitiva, cal millorar la definició dels criteris i terminis de conservació de la documentació i dur a terme les accions de la destrucció antiga que hagi superat els terminis definits de conservació.

6. CONCLUSIONS

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

ÀREES DE MILLORA
I – BLOC GENERAL
5.1. Auditoria. 5.2. Registre d'activitats del tractament. 5.3. Definició de les mesures per part del responsable del tractament. 5.4. Delegat de protecció de dades. 5.5. Encarregats del tractament i proveïdors sense accés a dades. 5.7. Drets de les persones interessades.
II – BLOC DE MESURES DE SEGURETAT
5.24. Criteris d'arxiu.
NO CONFORMITAT
I – BLOC GENERAL
5.6. Licitud del tractament, base jurídica, informació i consentiment.

Barcelona, 13 d'octubre de 2023.

Pere Ruiz Espinós

- Soci -

Caterina Bartrons Pou

- Gerent -