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-13.510

INDEX

1. OBJECTIUS I CONTINGUT

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

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

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

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

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

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

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

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

2. METODOLOGIA

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

Tant la planificació com el treball de camp d'auditoria, com també l'elaboració d'aquest informe, han estat desenvolupats per un equip de persones constituït per professionals qualificats en el camp de la protecció de dades de Faura-Casas, Auditors-Consultors, S.L. treballant de forma simultània els aspectes tècnics i organitzatius de la seguretat, així com també els legals.

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

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

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

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

3. DADES DE L'ENTITAT I TREBALLS EFECTUATS

3.1. DADES IDENTIFICATIVES

3.1.1. Dades Entitat

Entitat	Fundació Institut 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 centre de recerca públic localitzat a Badalona (Barcelonès). A nivell jurídic, és una fundació de dret privat que pertany al sector públic, perquè 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 realitzat els treballs de camp de l'auditoria en diversos departaments i serveis de l'entitat:

- Coordinadora de protecció de dades
- Delegat de protecció de dades
- Gerència
- Àrea de laboratori
- Àrea informàtica
- Àrea de recerca competitiva
- Àrea de gestió i finances
- Àrea de serveis generals
- Àrea de comunicació
- Àrea d'innovació
- Àrea de recursos humans
- Àrea de captació de fons
- Comitè d'ètica d'investigació clínica (CEIC)
- Biobank
- Unitat polivalent de la investigació clínica (UPIC)
- Centre de medicina comparativa i bioimatge (CMCIB)
- Àrea de plataformes
- Àrea de recerca
- Àrea de laboratori

S'han aportat i recollit informacions i evidències documentals suficients per a l'elaboració d'aquest informe d'auditoria.

3.2.1. Data de realització de l'auditoria

Data	1 i 2 de Juliol de 2021

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	Coordinadora de protecció de dades (CPD)
2	Carles Esquerré	Gerent
3	Lluís Sabaté	Representant de TIC Salut i Social, Delegat de Protecció de Dades (DPD), i representant al Comitè d'Ètica

4	Natàlia Ruiz	Lab Manager
5	Rubén Cobo	Cap de la unitat de tecnologia de la informació
6	Tadeo Lava	Enginyer a la unitat de tecnologia de la informació
7	Óscar Fraile	Cap de projectes competitius
8	Eva Garcia	Cap de finances
9	Àngels Serra	Responsable de gestió de clients
10	Paula Amorín	Gestió de proveïdors
11	Joaquim Puig	Cap de serveis generals
12	Roser Montserrat	Responsable de comunicació
13	Harvey Evans	Tècnica de comunicació
14	Raül Zurita	Cap d'innovació
15	Montse González	Cap de la unitat de gestió de persones
16	Anna Duran	Responsable de mecenatge
17	Sílvia Andrade	Responsable de gestió econòmica del mecenatge
18	Àngels Fortes	Secretària tècnica del Comitè d'Ètica (CEIC)
19	Magí Farré	President del Comitè d'Ètica (CEIC) i responsable de la unitat polivalent d'investigació clínica (UPIC)
20	Laia Pérez	Coordinadora del Banc de Tumors
21	Verónica Guirao	Coordinadora del Biobanc
22	Ana María Barrio	Coordinadora de la unitat polivalent d'investigació clínica (UPIC)
23	Patricia Fichado	Administració i secretària tècnica del CEIC i Bioseguretat.
24	Sra. Sara Capdevila	Directora tècnica Centre de medicina comparativa i bioimatge (CMCIB)
25	Carolina Gálvez	Coordinadora de les plataformes
26	Marcos Fernández	Responsable de la plataforma de citometria
27	Maria Pilar Armengol	Responsable de la plataforma de genòmica i microscòpia
28	Elisa Martró	Investigadora principal
29	Anna Carreras	Laboratori Manager GCAT Lab

30	José Domínguez	Investigador principal
31	Irene Latorre	Investigadora principal

Relació de la documentació lliurada a l'auditor:

- Conveni de cooperació amb l'Institut Català de la Salut (gerència territorial metropolitana nord) i la Fundació TIC Salut i Social per a la provisió de serveis de DPD, entre d'altres qüestions.
- Registre Activitats Tractament IGTP v2.
- Consentiment per a la utilització de material biològic sobrant v10.
- Contracte d'encarregat del tractament amb Bifor Seguretat, S.L. (seguretat i videovigilància).
- Contracte d'encarregat del tractament amb JDA Expert Legaltax, S.L.P. (assessorament professional de tipus legal, laboral, econòmic-financer, fiscal i comptable).
- Contracte d'encarregat del tractament amb Butler Scientifics, S.L. (anàlisi de dades biomèdiques).
- Contracte d'encarregat del tractament en què IGTP actua com a encarregat del tractament de les dades del client Aptatargets, S.L. (serveis de ressonància magnètica).
- Contracte amb la Fundació Institut Hospital del Mar d'Investigacions Mèdiques (IMIM) per a la realització d'assaig clínic: "Utilización de un adhesivo de fibrina para disminuir la dehiscencia de la anastomosis esofagoyeyunal en gastrectomies totales por càncer: estudio aleatorizado y multicéntrico".
- Material transfer agreement between IGTP (provider) and the University of Massachusetts Medical School (recipient).
- Material transfer agreement between Gilead Sciences, Inc. (provider) and IGTP (recipient).
- Material transfer agreement between IGTP (provider) and GCAT Project (recipient).
- Presentacions sobre protecció de dades realitzades per la CPD com a formació per al personal.
- Exemple clàusules (addicionals al contracte amb el personal).
- Modelo datos personales IGTP v.5. (adreçat al personal inclou informació sobre el tractament, d'acord amb l'art. 13 RGPD).
- Manual de bienvenida IGTP (adreçat al personal, inclou unes bones pràctiques).
- Vigilancia de la salud (personal).
- Accés a la Biblioteca de Ciències de la Salut de Catalunya (BCS) i autorització per a la cessió de les dades.
- Acta información investigador y técnico (acta de lliurament de documentació sobre prevenció de riscos laborals al personal). Documentació que es lliura al personal en el moment de l'acollida:
    - 0. Política preventiva de la empresa

- 1. Manual básico PRL
- 2. Extracto riesgos puesto de trabajo personal investigador
- 3. Normas de Seguridad en Laboratorio.
- 4. Extracto medidas de emergència
- 5. Uso de extintores
- 6. Pauta primeros auxilios
- 7. Accidentes in itinere.
- 8. Manipulación manual de cargas.
- 9. Orden y limpieza.
- 10. PVD Pantallas.
- 11. Exposición agentes biológicos.
- 12. Identificación agentes químicos.
- 13. Recomendaciones Trabajo laboratorio.
- 14. EPIS.
- 15. Normativa post-Covid.

- Circular 1 calculadora vacances i dies personals (personal).
- Manual portal del empleado (personal).
- Nota informativa (al personal) sobre terminis de presentació dels comunicats de baixa, alta i comunicats de confirmació per incapacitat temporal.
- Test curso inicial IGTP (prevenció de riscos per al personal).
- Medidas de seguridad (comunicat tècnic).
- Condiciones de uso de la infraestructura informática de la Institución.
- Copias de seguridad de la configuración de los dispositivos de red de IGTP-IJC.
- Configurar autenticación multifactor en office365.
- Copias de seguridad.
- Correo.
- Esquema red IGTP.
- Manual SelfService (comunicat tècnic).
- Manual Bienvenida de IT.
- Normativa de uso del correo electrónico IGTP.
- Política de seguridad de ficheros (comunicat tècnic).
- Prevenció davant d'atacs de phishing.
- Welcome pack (política de creació d'usuaris com a comunicat tècnic).
- Informes d'auditories internes RGPD de 21/03/2019 i 18/12/2020.
- AIPD registre de Riscos IGTP.
- Informe d'avaluació d'impacte IGTP.
- Informe d'avaluació d'impacte IGTP.

- Procediment AIPD IGTP.
- Drets Afectats.
- Guia drets dels Interessats.
- Procediment Drets dels Interessats.
- Registre sol·licituds dels interessats (document Excel).
- Formulari notificació incidència seguretat interessat.
- IGTP Registre d'Incidències de Seguretat de Dades (document Excel).
- Procediment de Violacions de Seguretat de Dades Personals.
- Formulari del DPD.
- Rebut de sol·licitud a l'APDCAT.

4. SIMBOLOGIA

En aquest informe s'hi analitzen tots els punts requerits per la normativa de protecció de dades. En cadascun d'aquests punts s'hi descriu quina és la situació actual, és a dir, la situació en el moment de la realització dels treballs de camp de l'auditoria, i quina és l'àrea de millora o no conformitat detectada, que s'il·lustra amb la simbologia següent:

Símbol	Significat
▲	**No detectada**, és a dir, la situació actual de l'Entitat compleix la normativa.
●	**Àrea de millora**, és a dir, l'estat de la situació actual requereix ésser completat perquè no s'ajustaria íntegrament a l'establert a la normativa.
▼	**No conformitat**, és a dir, la situació actual incompleix la normativa i ha de ser modificada de forma prioritària segons les recomanacions efectuades en l'Informe.

5. ANÀLISI DE LES DIFERENTS ÀREES DE L'AUDITORIA

I - BLOC GENERAL

5.1. AUDITORIA

Base legal: Article 24.1 RGPD

Situació actual

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

S'aporten evidències d'auditories realitzades a nivell intern sobre aspectes organitzatius, com són els documents titulats "*Informe d'Avaluació RGPD IGTP*", que porten dates 21/03/2019 i 18/12/2020. Aquests documents evidencien una anàlisi correcta de la situació de l'entitat i l'adopció de mesures correctores, però és necessària l'adopció d'una política de realització d'auditories externes biennals que tinguin caràcter exhaustiu.

Àrees de millora

●	Cal que l'entitat implementi una política de realització d'auditories sobre protecció de dades cada dos anys. També és necessari que es deixi constància de l'elevació del resultat de l'auditoria a la direcció i des les accions impulsades en conseqüència.

5.2. REGISTRE D'ACTIVITATS DEL TRACTAMENT

Base legal: Article 30 RGPD

Situació actual

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

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

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

- 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

El RAT ha estat elaborat com a document Excel. 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, etc.), a més d'altres informacions addicionals que contribueixen a la definició i comprensió dels tractaments, com ara les bases jurídiques aplicables en cada cas.

D'acord amb la disposició final onzena de la LOPDGDD, que modifica l'article 6 bis de la Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern, els subjectes del sector públic citats a l'article 77.1 de la LOPDGDD tenen l'obligació addicional de publicar el seu RAT i fer-lo accessible electrònicament. L'entitat, però, no es troba entre els subjectes obligats de l'article 77.1 de la LOPDGDD.

Àrees de millora

●	El RAT elaborat per l'entitat reflecteix i identifica de forma correcta els tractaments realitzats i s'ajusta fonamentalment a les previsions de l'art. 30 RGPD. Tenint en compte els diferents serveis i activitats que realitza l'entitat, constatem que totes aquestes activitats apareixen reflectides correctament al RAT. Com a elements de millora, indiquem alguns aspectes que poden tenir-se en compte: • Drets dels interessats: No cal incloure aquest apartat dins el RAT. Tot i que es constata que s'ha fet una reflexió sobre quins drets serien aplicables a cadascun dels tractaments, recomanem treure aquest apartat del RAT a fi d'evitar confusions. • Destinataris de les dades: Cal incorporar un camp de destinataris de les dades, d'acord amb l'art. 30.1.d) RGPD. És a dir, en relació a cada tractament, cal que el RAT inclogui un camp on es facin constar les categories d'organitzacions o persones a qui es comuniquin dades fora de l'entitat de forma habitual, si és el cas. • Transferències internacionals de dades. Cal fer constar també, respecte a cada tractament, si hi ha o transferències internacionals de dades. • Videovigilància. En haver-hi un tractament de dades de videovigilància, caldria que constés específicament al RAT.

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: "*Medidas de seguridad*", "*Condiciones de uso de la infraestructura informática de la Institución*", "*Copias de seguridad de la configuración de los dispositivos de red de IGTP-IJC*", "*Configurar autenticación multifactor en office365*", "*Copias de seguridad*", "*Correo*", "*Esquema red IGTP*", "*Manual SelfService*", "*Manual Bienvenida de IT*", "*Normativa de uso del correo electrónico IGTP*", "*Política de seguridad de ficheros*", "*Prevenció davant d'atacs de phishing*" i "*Welcome pack*.

La majoria d'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 les informacions proporcionades, es corresponen en bona part amb les que ja preveia l'antic Reglament de 2007 (RLOPD) que desenvolupava la LOPD anterior. Tot i que estem parlant d'una normativa que ja no és la referent, les mesures de seguretat que hi apareixien definides continuen essent vàlides. El RGPD no impedeix que les mesures de seguretat previstes pel RLOPD continuïn aplicant-se a fi de garantir el compliment de les obligacions del responsable del tractament. D'aquesta manera, l'entitat continua aplicant les mesures de seguretat citades, previstes al RLOPD, a més de voler complir els nous requeriments del RGPD, com ara el nomenament del DPD o l'elaboració d'un RAT, entre d'altres.

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

MESURES ORGANITZATIVES	
Deure de confidencialitat i secret	Evitar l'accés de persones no autoritzades a les dades personals: evitar pantalles desateses, documents en zones d'accés públic, etc. Quan s'absenti del lloc de treball es procedirà al bloqueig de l'estació o tancament de la sessió.
	Els documents en paper i suports electrònics s'emmagatzemaran en lloc segur (armaris, calaixos o espais d'accés restringit).
	No es llençaran documents o suports electrònics amb dades personals sense garantir-ne la destrucció.
	No es comunicaran dades personals o qualsevol informació personal a tercers.
	Signar amb els treballadors que tinguin accés a dades un acord de confidencialitat i entregar-los un manual per a usuaris amb les obligacions i mesures establertes.
	El deure de secret i confidencialitat es manté fins i tot després de finalitzar la relació laboral del treballador amb l'empresa.
Drets dels titulars de les dades	S'informarà als treballadors, sobretot als que puguin estar de cara al públic, sobre el procediment d'atenció als drets dels interessats, definint de forma clara els mecanismes previstos per a l'exercici d'aquests drets.
	Prèvia presentació del DNI o passaport, les persones interessades podran exercir els seus drets. El responsable del tractament haurà de donar d'atendre les seves peticions.
Violacions de seguretat de les dades	Quan es produeixin violacions de seguretat, es notificaran a l'autoritat de control en el termini de 72 hores d'ença del moment que se'n té coneixement. La notificació es realitzarà a través de la seu electrònica de l'autoritat de control.
	Es podrà gestionar de forma interna un registre d'incidències que es puguin produir amb dades personals.
Documentació paper	S'establiran criteris d'arxiu per a la documentació que contingui dades de caràcter personal, i es custodiarà de forma adequada, quan no es faci servir.
	Categories especials de dades: es restringirà l'accés a aquest tipus de documentació, s'habilitaran mètodes per a la seva

	destrucció i es durà a terme un registre d'accés a aquests documents.
Delegat de Protecció de Dades	✓ El tractament el realitzi una autoritat o organisme públic ✓ Les activitats consisteixin en operacions que, degut a la seva naturalesa, abast i/o fins, requereixin una observació habitual i sistemàtica d'interessats a gran escala. ✓ Les activitats principals consisteixin en el tractament a gran escala de categories especials de dades personals i de dades relatives a condemnes i infraccions penals.

MESURES TÈCNIQUES	
Identificació	S'establiran mecanismes d'autenticació personalitzats per accedir als sistemes mitjançant, per exemple, un usuari i contrasenya específics per a cada treballador (identificació inequívoca).
	S'establiran perfils d'usuaris amb diferents nivells d'accés a dades personals segons les funcions del treballador.
	Quan un dispositiu s'utilitzi per al tractament de dades personals i fins d'ús personal, es recomana establir perfils diferents.
	Es recomana disposar de perfils amb drets d'administració per a la instal·lació i configuració del sistema i usuaris sense privilegis.
	Es garantirà, com a mínim, l'existència de contrasenyes per a l'accés a les dades personals emmagatzemades als sistemes. La contrasenya tindrà almenys 8 caràcters (números i lletres) i l'empresa decidirà la complexitat d'aquestes claus. Es canviaran les claus, com a mínim, un cop l'any.
	Cal garantir la confidencialitat de les contrasenyes, evitant que puguin ser exposades a tercers.
	En cas de intents d'accés fallits a un compte d'usuari es bloquejarà aquest compte.
Deure de salvaguarda	Els dispositius i ordinadors utilitzats per a l'emmagatzemament i el tractament de les dades personals hauran de mantenir-se actualitzats.
	En aquests dispositius es disposarà d'un sistema d'antivirus

	instal·lat i degudament actualitzat.
	Per evitar accessos remots indeguts a les dades personals es prendran les mesures corresponents com l'existència de Firewall.
	Periòdicament (mínim setmanal) es duran a terme processos de còpia de seguretat de les dades personals en un suport diferent al que s'utilitza per al treball diari. Es disposarà d'una còpia de seguretat en un lloc diferent d'on s'emmagatzemen les dades.
	Categories especials de dades: es durà a terme un registre d'accessos d'aquest tipus de dades.
Gestió de suports i dispositius	Es disposarà d'un inventari actualitzat dels diferents suports/dispositius que continguin dades personals.
	Categories especials de dades: quan calgui realitzar l'extracció de dades personals fora del recinte on se'n fa el tractament, ja sigui per mitjans físics o electrònics, s'haurà de valorar la possibilitat d'utilitzar un mètode d'encriptació.
	S'establiran mecanismes de restricció d'accés a la sala on es trobin els servidors (CPD).
	Com a norma general, els fitxers que continguin dades personal s'emmagatzemaran en un servidor de fitxers i no en els dispositius dels usuaris de forma local.

El compliment d'aquestes mesures mínimes serà avaluat profusament en diferents punts d'aquest informe.

Els tractaments que realitza l'entitat a data de l'auditoria són, en gran part, els mateixos que realitzava anteriorment a l'entrada en aplicació del RGPD el 25 maig de 2018, de manera que les mesures de seguretat ja van ser definides i implementades sota l'anterior règim legal, tenint en compte les característiques i els riscos d'aquests mateixos tractaments.

Els diferents 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 preveu aplicar-hi. Del seu contingut pot inferir-se també que l'entitat ha analitzat i tingut en compte riscos del tractament.

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

Els informes d'auditories internes sobre RGPD de dates 21/03/2019 i 18/12/2020 demostren i evidencien que s'han tingut en compte els riscos que impliquen les activitats de tractament de dades i que s'han implementat mesures de seguretat en relació a aquests riscos. Aquestes mesures, tal com estan definides i plantejades, responen en bona mesura a les que ja preveia l'antic RLOPD i resulten adequades. En tot cas, caldrà que 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.

Constatem l'evidència d'haver-se realitzat models documentals per a la realització d'anàlisis de riscos i avaluacions d'impacte. Aquests models són correctes, perquè permetrien realitzar les corresponents anàlisis i avaluacions d'impacte, però fins ara no s'han aplicat concretament a cap tractament. Al RAT podem comprovar que, respecte a cadascuna de les activitats del tractament, s'ha indicat que no requereix una avaluació d'impacte. No obstant, caldria establir una previsió o valoració argumentada sobre la necessitat legal de fer avaluacions d'impacte en cada cas. Cal tenir en compte que determinades activitats de recerca impliquen el tractament de dades sensibles i l'ús de noves tecnologies i aplicacions, cosa que pot implicar riscos evidents per a les dades de les persones. Des de TIC Salut i Social, s'ha proporcionat als investigadors una eina específica per a la realització d'avaluacions d'impacte.

Finalment, cal fer notar l'obligació que tenen les entitats del sector públic o vinculades al servei públic d'aplicar les mesures de seguretat de l'Esquema Nacional de Seguretat (ENS), d'acord amb la disposició addicional primera de la LOPDGDD. L'entitat no es troba dins els supòsits d'entitats obligades, però cal tenir en compte que l'eina facilitada per TIC Salut i Social per a la realització d'avaluacions d'impacte ja té en compte els paràmetres i requeriments definits a l'ENS a l'hora d'establir mesures de seguretat aplicables.

Àrees de millora

●	En general, s'aporten documents de seguretat i protocols que demostren i evidencien l'adopció i aplicació per part de l'entitat de mesures de seguretat adequades. La major part de la documentació aportada s'ajusta a criteris de seguretat i de compliment legal; presenta un format i validació oficials per part del responsable del tractament. Cal fer sempre una revisió de les mesures de seguretat i circuits existents per tal de corroborar que són adequats als requeriments legals del RGPD; en particular, cal prioritzar els principis de privacitat per disseny i per defecte en les mesures de seguretat i circuits de tractament que s'estiguin aplicant. Tot i que l'entitat ja compta amb un procediment definit per a la realització d'avaluacions d'impacte, com a àrea de millora es pot considerar la realització d'una valoració específica i argumentada sobre si hi pot haver la necessitat legal de realitzar una avaluació d'impacte en cada activitat de tractament, sobretot en relació a tractaments que impliquin un alt nivell de risc per als drets i llibertats de les persones, també especialment quan es pretengui aplicar noves tecnologies en el seu tractament, de conformitat amb l'art. 35 RGPD i els criteris de la llista de tractaments especificats per l'AEPD. Hem d'entendre tot això també vinculat a l'obligació que té l'entitat de gestionar el risc en general i el principi de

	responsabilitat proactiva. Les autoritats de control han publicat guies sobre criteris i metodologia a emprar en l'anàlisi de riscos i l'elaboració d'avaluacions d'impacte, tant l'Agència Espanyola de Protecció de Dades (AEPD) com l'Autoritat Catalana de Protecció de Dades (APDCAT). També recentment l'AEPD ha publicat una eina online sobre la matèria que s'anomena GESTIONA. Degut a la complexitat d'aquests informes, el més habitual és encarregar-ne l'elaboració a empreses o entitats especialitzades, sota la supervisió del DPD de l'entitat. D'altra banda, cal recordar que, si bé el DPD ha de col·laborar-hi, no seria correcte que fos el DPD o CPD qui elaborés directament els informes d'avaluació d'impacte, ja que això plantejaria problemes de compatibilitat amb les seves altres funcions d'assessorament i supervisió.

5.4. DELEGAT DE PROTECCIÓ DE DADES

Base legal: Article 37 RGPD

Segons la informació i evidències proporcionades, l'entitat va procedir en un moment anterior a nomenar la Sra. Iris Bargalló com a delegada de protecció de dades (DPD). Aquest nomenament es va notificar a l'Autoritat Catalana de Protecció Dades.

Actualment, d'acord amb el conveni el passat signat el 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 i revisat convenientment, 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. L'antiga DPD de l'entitat assumeix les funcions de Coordinadora de Protecció de Dades (CPD), que també té unes funcions definides dins aquest nou marc de relacions.

D'acord amb aquest model de DPD del sector públic sanitari, 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.

D'acord amb les informacions i documentació proporcionades, podem corroborar que ja s'han realitzat accions de difusió i formació al personal (sobretot, a personal investigador i d'administració) relatives a protecció de dades sota la coordinació de la CPD. Les presentacions aportades constitueixen una evidència d'aquesta activitat proactiva. En aquest sentit, s'ha fet una correcta difusió de la figura del DPD actual. Confirmem que, en general, els textos legals que fa servir l'entitat per a informar sobre el tractament de les dades, de conformitat amb l'art. 13 RGPD, ja estan actualitzats i informen també sobre l'existència del DPD actual i la forma de comunicar-s'hi.

A la base de dades pública sobre delegats de protecció de dades, accessible a través de la web de l'AEPD, constatem que a data de l'auditoria encara hi consta com a DPD la Sra. Iris Bargalló i no pas l'entitat TIC Salut i Social. D'acord amb les informacions proporcionades durant la realització de l'informe, però, ja s'han iniciat els tràmits per a actualitzar aquest registre, a fi que hi consti el DPD vigent, que és el del sector públic sanitari de Catalunya.

Comprovem que la figura del DPD no apareix a l'organigrama de l'entitat, que, d'acord amb les informacions proporcionades, podem observar a la web corporativa.

L'entitat no té un Comitè de Seguretat o similar que tracti temes de protecció de dades, però el delegat de protecció de dades té presència al Comitè d'Ètica. Tot i que no hi ha una previsió d'informació regular a la direcció de l'entitat per part de la CPD, el contracte signat amb el DPD preveu diferents mecanismes d'informació, com ara un informe anual que la CPD ha de proporcionar al DPD, i la necessitat que el DPD informi també la direcció de l'entitat sobre la seva activitat.

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.

Àrees de millora

●	Cal fer seguiment del tràmit d'actualització de les dades del DPD a l'APDCAT i comprovar que finalment hi apareix el DPD actual de l'entitat. Malgrat no haver-hi una obligació expressa, com a mesura de difusió del seu nomenament recomanem que s'incorpori la figura del DPD en organigrames que faci servir l'entitat.

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 les persones o empreses externes a qui permet un accés autoritzat a les seves dades, i té signats contractes d'encàrrec de tractament amb totes elles. No obstant, aquest control no està centralitzat, sinó que depèn de diferents àrees de l'organització i del tipus de contracte. Els contractes de recerca són revisats per l'advocada i, si impliquen tractament de dades, es proporcionen a la CPD per a la seva revisió. En el cas dels contractes de compres, segueixen processos de licitació i tenen els seus propis assessors legals.

Comprovem que l'entitat disposa d'un model de contracte d'encàrrec de tractament de dades degudament actualitzat i ajustat al RGPD.

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

ET DETECTATS	SERVEI PRESTAT	CONTRAC-TE	COMENTARIS
Bifor Seguretat, S.L.	Seguretat i videovigilància	✓	El contracte signat és conforme al RGPD.
JDA Expert Legaltax, S.L.P.	Assessorament professional de tipus legal, laboral, econòmic-financer, fiscal i comptable	✓	El contracte signat és conforme al RGPD.
Butler Scientifics, S.L.	Anàlisi de dades biomèdiques	✓	El contracte signat és conforme al RGPD.

D'altra banda, també revisem un contracte d'encarregat en què IGTP actua com a encarregat del tractament de les dades del client Aptatargets, S.L. (serveis de ressonància magnètica). Aquest contracte també és conforme al RGPD i, per tant, està actualitzat i ajustat a la normativa.

Com a exemple de contracte per a la realització d'un assaig clínica, revisem el corresponent al projecte: "*Utilización de un adhesivo de fibrina para disminuir la dehisecencia de la anastomosis esofagoyeyunal en gastrectomies totales por càncer: estudio aleatorizado y multicéntrico*". Aquest contracte ja conté previsions sobre protecció de dades que tenen com a referència i apliquen la normativa vigent. Aquestes previsions també determinen un règim de corresponsabilitat en el tractament de les dades i estableixen les obligacions de confidencialitat i diligència que corresponen a cadascuna de les parts.

Els contractes MTA ("material transfer agreements") signats amb University of Massachusetts Medical School (receptora), Gilead Sciences, Inc. (proveïdora) i GCAT Project (receptora) també contenen previsions adequades sobre confidencialitat i seguretat en la transferència dels materials des del punt de vista de protecció de dades.

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

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

Àrees de millora

●	Tot i que els contractes revisats són correctes, l'absència d'un control centralitzat sobre els encàrrecs de tractament, o més ben dit, l'existència de controls legals diferents en funció del tipus de contracte pot portar a l'existència de proveïdors que tinguin accés a les dades sense que hi hagi un contracte actualitzat. Per això, com a millora, recomanem disposar d'un control i seguiment centralitzat a l'organització de tots els proveïdors que tinguin o no un accés a dades i del contracte d'encàrrec de tractament que han de signar o no. Tots aquests proveïdors/encarregats del tractament haurien de constar en un únic document per al seguiment o actualització d'aquests contractes d'encàrrec, en cas necessari. També com a millora, cal disposar d'un protocol específic que inclogui les previsions de l'entitat sobre encarregats del tractament i sobre la manera de seleccionar-los i relacionar-s'hi, a fi de garantir que apliquen les mesures de seguretat necessàries.

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 disposa d'una una mostra de compromisos de confidencialitat signats que pugui aportar. Tanmateix, comprovem que hi ha un seguit de serveis que es presten per empreses externes, com ara serveis de neteja o manteniment. Els processos de contractació d'aquests proveïdors es fa des de l'àrea de Compres, que disposa dels seus propis assessors legals, diferents dels responsables de protecció de dades.

És probable que els processos de contractació dels proveïdors de serveis que han de tenir un accés autoritzat a les instal·lacions ja incloguin previsions de confidencialitat i seguretat. No obstant, seria convenient que restessin dins l'àmbit de control i seguiment dels responsables de protecció de dades de l'entitat.

Àrees de millora

●	Com en l'apartat anterior, seria recomanable que els responsables de protecció de dades disposessin d'un únic document per a tota l'entitat on poguessin fer seguiment dels diferents proveïdors i així poder decidir en cada cas si els correspon signar un contracte d'encàrrec de tractament o un compromís de seguretat. D'aquesta manera, també es podria comprovar efectivament que els instruments jurídics més adequats són els que s'apliquen en tot moment i que no resta cap proveïdor al marge d'aquest control.

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 diferents activitats de tractament de dades que du a terme l'entitat i que es fan constar al RAT:

- Treballadors
- Treballadors de contractes
- Visitants
- Treballadors d'empreses que lloguen espais dins l'IGTP
- Membres del CEIC
- Clients
- Rescabalaments
- Proveïdors
- Amics de Can Ruti
- Comunicació
- Investigadors
- GCAT
- Plataformes: Genòmica, Genòmica Translacional, Microscopia, Proteómica
- Biobanc
- Donants Econòmics
- Participants UPIC
- Pacients Proves Diagnòstiques
- Grups d'Investigació
- Neurogenètica

- **Treballadors / Investigadors**

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

  L'entitat compta amb una plantilla aproximada de tres-cents treballadors en règim laboral, a temps complet o a temps parcial, a més de quatre-cents treballadors adscrits que provenen d'altres institucions amb qui té un conveni signat (per exemple, l'ICO Badalona, l'Hospital Germans Trias i Pujol o l'Institut Josep Carreras).

  Des de l'àrea de recursos humans de l'entitat participen activament en processos de selecció de personal. En general, a cada àrea defineixen el perfil del candidat i a recursos humans fan difusió de l'anunci a través de LinkedIn, Escola d'Infermeria, Biocat o la pròpia web. Sempre que es reben currículums es reben a través de correu electrònic, i ja està previst proporcionar una informació sobre protecció de dades que és conforme a l'art. 13 RGPD, tal com podem comprovar. Cal tenir en compte que els perfils requerits són sovint molt especialitzats i que els processos de contractació han de seguir parcialment criteris de contractació pública. Això fa que els currículums s'hagin de guardar de forma indefinida, a efectes de poder acreditar que els processos han

respectat els criteris definits per les normatives de transparència i contractació pública. Seria recomanable revisar aquesta política vigent de l'entitat i determinar de forma més clara quin és el criteri de conservació, ja que hi ha d'haver un criteri o termini de conservació de currículums que estigui definit.

L'elaboració de les nòmines i la gestió laboral en general està encarregada a la gestoria JDA Expert Legaltax, S.L.P., amb la qual, tal com hem pogut comprovar, ja hi ha un contracte d'encàrrec de tractament de dades.

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

- Informacions diverses sobre prevenció de riscos
- Instruccions d'accés al domini
- Informació sobre protecció de dades, d'acord amb l'article 13 RGPD.

D'altra banda, d'acord amb les informacions i evidències proporcionades, comprovem també que, juntament amb el contracte de treball, es fan signar els següents documents, que el treballador pot decidir signar o no:

- Consentiment exprés per a l'ús de la imatge
- Compromís de confidencialitat
- Compromís sobre prevenció de riscos
- Compromís de compliment de bones pràctiques en l'ús de les eines informàtiques.

Corroborem que la informació legal que es proporciona al personal sobre protecció de dades tant en el procés d'acollida com en el moment de signar el contracte de treball és ajustada a l'obligació d'informar sobre el tractament de les dades, d'acord amb l'art. 13 del RGPD.

Segons les informacions proporcionades, el sistema que es fa servir a l'entitat per al fitxatge es gestiona des d'una empresa externa, però ara com ara no hi ha un sistema de registre de la jornada laboral. Està prevista, però, la propera implementació d'un sistema de control de jornada a través d'una app mòbil o per una programa instal·lat a l'ordinador.

En general, el personal laboral gestiona les seves pròpies dades i alguns elements de la relació laboral, com ara les vacances i els permisos, des de la intranet corporativa.

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 finalitats de divulgació o comunicació de l'entitat, es tindria en compte el model de consentiment específic que s'ofereix al treballador en el moment de signar el contracte laboral i que pot decidir signar o no lliurement.

Pel que fa a la vigilància de la salut, és un servei que també li presta a l'entitat l'empresa MDP. També compta amb els serveis de la Mútua Intercomarcal.

Respecte a l'increment del teletreball com a conseqüència de la recent emergència sanitària causada per la Covid-19, l'entitat facilita diferents possibilitats d'accés remot als

sistemes: VPN, escriptori virtual i via web. No consta que hi hagi un protocol específic sobre accessos remots. Per aquest motiu, seria recomanable que l'entitat definís unes previsions per escrit sobre el teletreball, determinant quines garanties i mesures suposa des del punt de vista de la seguretat i la privacitat, i n'informés el personal de manera adequada.

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

- **Treballadors de contractes / Visitants / Treballadors d'empreses que lloguen espais dins l'IGTP / Membres del CEIC**

  Aquests tractaments responen a la finalitat de mantenir 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, també l'execució d'aquest contracte.

  En tots aquests tractaments, les dades que es recullen i es mantenen són les mínimes 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.

  No consta que hi hagi un instrument específic destinat a proporcionar una informació sobre aquests tractaments, d'acord amb l'article 13 RGPD, i per tant seria recomanable implementar un procediment pel qual aquesta informació es pogués proporcionar en els controls d'accessos, per exemple, a través de posar aquesta informació disponible en forma de cartell a la recepció.

- **Clients / Rescabalaments / Proveïdors.**

  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, també seria la preparació i execució d'un contracte.

  A l'àrea de gestió i finances de l'entitat es du a terme tota la facturació i comptabilitat de la institució. En particular, es facturen assajos clínics, serveis prestats a altres entitats clients (hospitals, serveis de recerca, diagnòstics, etc.) i cursos de formació patrocinats per laboratoris o hospitals. En general, les úniques dades que es recullen i conserven són les necessàries per a la facturació, ja que la majoria de serveis (també la formació patrocinada) no implica tractar altres dades. En els assajos clínics es paguen tickets dels participants o pacients; tanmateix, les dades es tracten sempre anonimitzades.

  Hi ha un grup de recerca de l'IGTP que fa un diagnòstic genètic com a servei que s'ofereix i es factura directament. En general, el client d'aquest servei és un hospital. A petició del client, s'inclou dins el tractament la sol·licitud de la prova genètica, que inclou les dades de la persona física, però això és innecessari i incorrecte. Caldria

implementar també dins aquest tractament, si és possible, mesures de seudonimització, per tal que no calgués identificar la persona física en la prestació del servei. No obstant, en aquest cas concret, cal tenir en compte que el responsable del tractament és qui pot decidir, en darrera instància, quines són les mesures de seguretat que s'han d'aplicar.

Pel que fa a la facturació rebuda, 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.

Hi ha un proveïdor de serveis de ressonància magnètica que inclou els noms de les persones a qui es fa la ressonància. Si bé la informació s'envia codificada, com en el cas anterior, seria recomanable implementar procediments de seudonimització que fessin innecessari la identificació de les persones en la prestació dels serveis.

- **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, es fonamenta jurídicament, de manera general, en l'obtenció del consentiment de l'interessat, que pot revocar en qualsevol moment.

D'acord amb les informacions proporcionades, l'entitat du a terme diferents activitats de recerca molt diferenciades i, per això, s'ha optat al RAT per diferenciar-les com a tractaments també diferents, si bé coincideixen en gran mesura en la finalitat i la base jurídica. En general, els investigadors principals són els encarregats de sol·licitar accessos a les eines informàtiques i als recursos necessaris per a cada projecte.

Tots els projectes de recerca i els assajos clínics requereixen una avaluació prèvia per part del Comitè d'Ètica d'Investigació Clínica (CEIC) de l'entitat, el qual està conformat per una secretària tècnica, un president i un representant del DPD. En molts casos, el responsable del tractament és un hospital, però això no evita de cap manera que tots els projectes passin per aquest procediment, sempre que impliquin d'alguna manera el tractament de material humà. El CEIC fa una valoració científica, ètica i legal de cada projecte i emet finalment un dictamen, que pot ser favorable o denegatori, o pot demanar correccions i/o aclariments.

Segons les informacions proporcionades, s'apliquen habitualment mesures de seudonimització des del moment que les dades són recollides. A aquest efecte, es té en compte la Guia de TIC Salut i Social per a decidir quan les dades han de ser "identificatives" o han de seudonimitzar-se. En particular, comprovem que el projecte de la Dra. Elisa Martró per a la millora de l'accés al diagnòstic de les persones aplica procediments de seudonimització que eviten que els investigadors tinguin accés a les dades que permeten identificar les persones.

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 seudonimització, 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 seudonimització.
- Compromís de confidencialitat i de no fer cap activitat de reidentificació signat per l'equip investigador.
- Aplicació de mesures per evitar la reidentificació.

Com a suport important de l'activitat de recerca, l'entitat compta amb un Biobank, que emmagatzema materials biològics, aplicant criteris d'utilitat pública. Les mostres s'identifiquen a través de codis i es gestionen de manera seudonimitzada. El Biobank disposa d'un model de consentiment, que s'ajusta a la normativa sobre protecció de dades.

També com a suport a la recerca, l'entitat disposa d'una Unitat Polivalent d'Investigació Clínica (UPIC), que presta serveis de manera transversal a tots els investigadors, especialment de personal d'infermeria, de administració i de farmacologia. Cada estudi 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.

Si bé la majoria de participants 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 de futurs estudis.

Un altre servei rellevant que presta l'entitat com a suport a la recerca biomèdica és el que deriva del Centre de Medicina Comparativa i Bioimatge (CMCIB). En aquest cas, tota gran part de l'activitat científica es du a terme amb animals i és pre-clínica, llevat del servei de diagnòstic per la imatge. En el cas de les ressonàncies magnètiques, es gestionen de manera seudonimitzada. Totes les mostres de materials humans que pugui tractar el CMCIB també arriben seudonimitzades.

Les plataformes de citometria, genòmica i microscòpia suposen la prestació de tecnologies avançades no només a l'entitat, sinó a la comunitat científica en general. En aquest cas, d'acord amb les informacions proporcionades i les evidències aportades, la gestió de les mostres també es fa de manera seudonimitzada.

És important tenir en compte l'abast d'alguns projectes i allò que poden implicar des del punt de vista de protecció de dades. D'una banda, cal tenir en compte que hi ha projectes que poden implicar transferències internacionals a països "no segurs". Comprovem que un dels projectes analitzats implica transferència de dades seudonimitzades a Xile. D'acord amb les informacions proporcionades, però, la transferència ja està degudament legitimada a les clàusules contractuals. D'altra banda, hi ha projectes, com el GCAT, que impliquen el tractament de dades de categoria especial a gran escala, la qual cosa és indicativa de riscos manifestos per als drets de les persones. En projectes com aquest i en projectes de recerca en general, cal comprovar si

hi concorre o no la necessitat legal de fer una avaluació d'impacte de forma prèvia. En cas que es determini que no hi ha aquesta necessitat legal, recomanem que es deixi constància dels motius que porten a aquesta decisió. En tot cas, el GCAT ja fa avaluacions d'impacte, tenint en compte que el Comitè d'Ètica pot requerir-les.

- **Comunicació / Amics de Can Ruti**

Aquests tractaments impliquen tractar les dades necessàries per tal de poder enviar o proporcionar informació sobre els serveis de l'entitat, amb finalitats promocionals o de fidelització. Mitjançant aquest tractament es poden recollir dades de persones que tenen interès en les activitats que porta a terme l'entitat i demanen informació, i d'aquesta manera poder-los donar resposta.

La comunicació interna amb el personal s'articula sobretot a través de la intranet corporativa, però també es fa servir el correu electrònic. D'acord amb les informacions proporcionades, es duen a terme habitualment diferents accions de comunicació interna.

La comunicació externa, d'altra banda, es fa a través de les xarxes socials (Twitter i LinkedIn) i la web corporativa. La gestió de xarxes socials, a través de les quals l'entitat informa sobre els seus serveis, no impliquen generalment un tractament de dades. Les xarxes que es fan servir habitualment són Twitter i LinkedIn. En cas que s'hagués de publicar-hi la imatge d'una persona treballadora o usuària de l'entitat, es comprovaria que prèviament ha prestat la seva autorització. Constatem que l'entitat fa servir models d'autorització per a l'ús de la imatge que s'adjunten al contracte de treball. Aquestes autoritzacions es recullen per defecte i informen sobre la finalitat de la recollida i l'ús de la imatge. En general, en compte de proporcionar per defecte el model de consentiment a tot el personal, seria més ajustat a les necessitats del tractament demanar que es signés l'autorització només en cas que realment s'hagués de fer servir la imatge de la persona treballadora, informant en el document de forma més clara sobre l'ús que es donarà a la imatge (per exemple, dir que es difondrà a través de les xarxes de comunicació de l'entitat i de la web corporativa).

Un altre vessant de la comunicació corporativa és la newsletter, que s'envia de forma periòdica i per mitjà de mailchimp a les persones que voluntàriament han prestat el seu consentiment a través d'un formulari de la web. Aquest formulari ja inclou un avís legal sobre protecció de dades, que és conforme a l'art. 13 RGPD. La newsletter ja inclou una opció que permet als seus receptors donar-se de baixa en qualsevol moment de forma immediata.

Pel que fa a la web, comprovem també 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 rebutjar l'ús de cookies de forma expressa i prèvia a la navegació.

Altres activitats de comunicació que pot dur a terme l'entitat són les relatives a l'organització de seminaris o jornades semipresencials. En aquests casos, tanmateix, ja està previst que els formularis d'inscripció incloguin els corresponents avisos legals sobre protecció de dades.

- **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.

Els donants poden ser persones físiques i poden fer les donacions a través de la plataforma web "Els amics de Can Ruti", que gestiona l'entitat. Comprovem que, en fer la donació, ja apareix juntament al formulari de recollida de dades un avís i política de privacitat que conté la informació sobre el tractament de les dades.

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

- **Videovigilància**

Aquesta activitat no figura al RAT, però comprovem que efectivament es du a terme per part del responsable del tractament. D'entrada, val a dir que, com a activitat diferenciada, hauria d'incloure's al RAT.

A través d'aquesta activitat de tractament es pot captar 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 legal d'aquest tractament seria el compliment d'una missió en interès públic, d'acord amb l'article 6.1.e) del RGPD. No consten usos de la videovigilància per a finalitats de control laboral o de qualsevol altre tipus.

Actualment, l'entitat disposa de diverses càmeres instal·lades en diferents punts d'accés. Les gravacions de les càmeres es troben controlades per l'externa Bifor Seguretat, amb qui l'entitat ja té un contracte d'encàrrec de tractament de dades signat. Només el personal de seguretat està autoritzat a accedir a les gravacions.

Les càmeres es troben instal·lades als accessos i porten incorporats cartells informatius sobre videovigilància, que són ajustats a la normativa. Les gravacions es conserven durant dos mesos i després es van sobreescrivint, però això no és correcte. D'acord amb la Instrucció 1/2006 de l'AEPD i la interpretació que n'ha fet posteriorment la mateixa AEPD en la seva Guia de Videovigilància, es manté el període màxim de conservació d'un mes. Per tant, és necessari assegurar-se que el període de conservació de les imatges no supera el mes.

El tractament descrit és correcte i no planteja problemes de legitimitat o licitud, a banda dels aspectes indicats. En termes generals, s'ajusta a la finalitat de seguretat.

Àrees de millora

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

5.7. DRETS DE LES PERSONES INTERESSADES

Base legal: Articles 13-23RGPD

Situació actual

L'entitat ja disposa dels models i ja té un procediment definit per a l'exercici dels drets de les persones interessades, tal com es pot comprovar amb les diferents evidències documentals aportades. En particular, el document "*Drets Afectats*" conté els formularis actualitzats per a l'exercici dels drets d'accés, rectificació, supressió, oposició, limitació i portabilitat. Per tant, ja està previst a l'entitat un procediment actualitzat i ajustat al RGPD per a l'exercici dels drets d'accés, rectificació, oposició, supressió, limitació del tractament i portabilitat de les dades. El document "*Procediment Drets dels Interessats*" descriu el procediment previst a l'entitat i el document titulat "*Guia drets dels Interessats*" constitueix una evidència de la difusió que s'ha realitzat internament sobre l'exercici dels drets.

En general, en tots els avisos legals 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.

Tot i que l'entitat disposa d'un registre en format Excel per a registrar l'exercici dels drets (aportat com a evidència a aquesta auditoria), no consten procediments tramitats formalment segons el procediment previst pel responsable.

De manera informal, les peticions d'accés a la informació s'atendrien a les diferents àrees de comunicació, de personal i de recerca per part dels responsables.

Encara que no hi hagi exercicis formals, s'han aportat suficients evidències de l'existència del procediment i de les seves característiques que permeten afirmar l'existència i vigència d'aquesta mesura, aplicada de conformitat amb la normativa.

No detectada

▲	

5.8. NOTIFICACIONS DE VIOLACIONS DE SEGURETAT

Base legal: Articles 24 i 33 RGPD

Situació actual

L'entitat aporta evidències i proporciona informació que acrediten l'existència d'un procediment previst de registre d'incidències i de notificació de violacions de seguretat. En concret, el document aportat "*Procediment de Violacions de Seguretat de Dades Personals*" descriu el procediment definit pel responsable del tractament. D'altra banda, s'han aportat també evidències documentals d'un model de formulari de notificació i d'un registre en format Excel.

D'acord amb el registre Excel aportat, es constata l'existència d'algunes incidències en el tractament de les dades que han estat comunicades i registrades per l'entitat, que serien la troballa d'unes factures a l'escàner i un errada en una comunicació. Les incidències registrades tenen un caràcter poc greu.

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

Segons les evidències i informacions proporcionades, es constata l'evidència d'accions de difusió i formació realitzades per la CPD que impliquen el personal en la comunicació d'incidències de seguretat, de conformitat amb el procediment previst. No obstant, un cop revisat el procediment d'acollida de nou personal i les instruccions que es donen al personal sobre seguretat en general, constatem que no s'ha difós o proporcionat de manera generalitzada al personal una instrucció específica sobre la necessitat de comunicar incidències de seguretat, cosa que planteja dubtes sobre l'eficàcia del procediment.

Àrees de millora

●	Tot i que ja hi ha previst un procediment i ja s'han fet accions de formació en relació a les incidències i violacions de seguretat, és important verificar que s'instrueix bé el personal (bé sigui a través d'un manual de bones pràctiques o per qualsevol altre mitjà, preferentment en el moment de l'acollida del nou personal) sobre la seva obligació de comunicar incidències de seguretat en el tractament de les dades al DPD o a la persona que es designi a través d'un procediment clarament definit. Cal que de forma centralitzada es registrin totes les incidències de seguretat i el tractament que se'ls ha donat.

5.9. DIFUSIÓ DE FUNCIONS I OBLIGACIONS

Base legal: Articles 24 i 25 RGPD

Situació actual

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

Tots els procediments d'acollida que se segueixen a l'entitat preveuen proporcionar per escrit instruccions fonamentals i directrius sobre protecció de dades ja des d'un moment inicial. En particular, el document "*Manual de bienvenida de IT*" conté un apartat titulat "*Buenas prácticas en el uso de las TIC de la institución*", que aplega diferents mesures de seguretat destinades al personal. D'aquesta manera, es garanteix un coneixement fonamental sobre mesures de seguretat, funcions i obligacions del personal en matèria de privacitat i seguretat. Aquests documents, d'altra banda, es troben disponibles a la intranet per a tot el personal.

En definitiva, resulta clar que s'estaria complint la necessitat de difondre les obligacions i les mesures de seguretat específiques que tot el personal ha de conèixer i aplicar. Només com a aspecte a millorar, tal com s'ha evidenciat en el punt anterior, es troba a faltar una definició del procediment de registre d'incidències i notificació de violacions de seguretat en les instruccions proporcionades durant els procediments d'acollida.

Àrees de millora

●	Tot i que procediment d'acollida previst per l'entitat ja preveu comunicar instruccions sobre seguretat, recordem que caldria difondre també l'obligació del personal de comunicar qualsevol incidència o violació de seguretat a la CPD, tal com hem comentat al punt anterior.

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 directori actiu, el correu electrònic, el SAP (per a planificació i control econòmic) i el programa NorayBanks (per al Biobank) a més d'altres entorns que puguin fer-se servir en determinades àrees.

Quan entra un nou membre del personal a l'entitat, des de Recursos Humans s'emplena un Excel definint el seu perfil d'accés (per exemple, indicant que és personal d'administració); els responsables d'informàtica obtenen la informació sobre el perfil que li han d'assignar d'aquest Excel i envien un primer correu electrònic al seu correu personal amb la informació necessària per a un primer accés autoritzat al domini de l'entitat; en aquest correu hi indiquen el nom d'usuari i la contrasenya provisional (el número de DNI), que haurà canviar obligatòriament durant el primer accés. El nom d'usuari consisteix generalment en la primera lletra del nom i el cognom.

De forma habitual, per a l'accés als entorns de tractament de dades, sempre es requereix la introducció de contrasenya unipersonal. Per a l'accés al domini i al correu electrònic, la contrasenya ha de complir determinats requisits de robustesa: no pot incloure el nom d'usuari, ha d'estar formada per un mínim de 8 caràcters i ha d'incloure majúscules, minúscules, números i/o caràcters especials (ha de complir 3 d'aquests 4 criteris sobre caràcters). A més, aquestes contrasenyes han de ser renovades necessàriament cada 180 dies i no poden repetir-se. En el cas de l'accés al SAP i al programa NorayBanks, que també tenen controls per usuari i contrasenya, les contrasenyes no presenten requisits de robustesa. No obstant, és important aclarir que el seu accés està vinculat a un accés previ al domini.

L'usuari del domini pot accedir a les carpetes de l'entorn informàtic que siguin necessàries per al desenvolupament de les seves tasques. El sistema estableix la diferència entre 2 unitats: administració i recerca.

També s'apliquen com a control d'accés als sistemes informàtics d'altres mesures de seguretat, com ara la limitació per intents d'accés fallits, que permet fins a 3 intents, després dels quals es bloqueja i només es pot bloquejar a través d'un procediment específic. En un primer moment, el bloqueig és temporal (15 minuts), però en cas d'un nou intent d'accés fallit, el bloqueig seria indefinit. D'altra banda, també s'aplica una mesura de seguretat de bloqueig per inactivitat, que preveu que, en cas de 10 minuts d'inactivitat, el sistema es bloquegi.

L'accés a internet està protegit per un Firewall perimetral Juniper, que filtra les entrades i sortides d'informació en relació a l'exterior, amb la intenció d'evitar possibles atacs que es produeixin des d'internet. D'altra banda, com a mesura de seguretat, l'entitat també té instal·lats a tots els equips informàtics el Firewall de Windows i un antivirus Kaspersky. Aquest antivirus es manté actualitzat.

Els accessos remots autoritzats per l'entitat es vehiculen a través de diferents sistemes: determinats empleats i els proveïdors externs accedeixen a la xarxa per VPN. En canvi, a determinats membres del personal, sobretot a partir de la pandèmia de Covid-19, se'ls ha habilitat un accés remot a través d'un sistema d'escriptori virtual.

El procediment per a donar de baixa com a usuari autoritzat un membre del personal es realitza a través de fer-ho constar a l'Excel sobre personal. Aquest Excel és el mitjà que es fa servir habitualment per a la comunicació entre les àrees de recursos humans i recursos informàtics per a la gestió i actualització dels accessos autoritzats als sistemes informàtics de l'organització. Aquesta comunicació sempre té lloc de forma immediata a la modificació o cessament en la prestació de serveis per part d'un treballador.

Es constata l'evidència de mesures de seguretat definides en documents específics i protocols i un text sobre bones pràctiques. En un manual de benvinguda d'IT que es proporciona al personal, ja s'hi preveuen instruccions sobre seguretat en el tractament de les dades. S'hi determina, entre d'altres, la necessitat de fer un bon ús de les eines informàtiques que l'organització posa a la seva disposició i de no guardar informació en local.

L'entitat ha adoptat mesures específiques davant l'increment significatiu del teletreball i les videoconferències com a conseqüència de les mesures destinades a prevenir contagis de Covid-19, però no s'ha desenvolupat un protocol específic. En general, totes les persones que utilitzen aquestes eines i recursos de forma autoritzada es troben sota el control de l'àrea d'informàtica.

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. L'entitat té un control i registre sobre les persones autoritzades que tenen claus per accedir a les instal·lacions i als despatxos. L'accés general a les instal·lacions ja disposa habitualment d'un control i registre d'accessos, tant de dia com de nit, que es fa a través del programa Amadeus amb la finalitat de poder saber quanta gent hi hauria dins les instal·lacions per motius de seguretat (en cas de ser necessària una evacuació, per exemple). En el cas de l'accés a determinades zones restringides, cada responsable de cada departament pot demanar-li al responsable de serveis generals que autoritzi l'accés de determinada persona a una àrea restringida. Aquest accés es fa a través de targetes. D'altra banda, també hi ha determinats accessos autoritzats que es fan a través de claus, i la informació sobre aquests accessos es troba registrada en un document Access.

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 pel personal autoritzat, que és personal d'informàtica, de serveis generals i de manteniment. Tant el CPD de mar com el de muntanya, com també el de l'àrea de Linux, són accessibles a través d'un control per targeta magnètica.

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. Els tres Centres de Processament de Dades (CPD) es troben en sales d'accés restringit, l'accés a les quals només és possible a través de targeta magnètica.

A banda de disposar d'un Firewall perimetral que controla les entrades i sortides d'informació, els equips informàtics també duen instal·lats el Firewall de Windows i un antivirus Kaspersky.

L'entitat autoritza accessos remots als seus sistemes a través d'escriptori virtual i de tecnologia VPN. Per a la connexió amb VPN es requereix la instal·lació als equips informàtics dels empleats d'un software específic. Per tant, ja s'hi apliquen mesures de control i actualització.

Els equips informàtics no porten bloquejats els ports, però el manual de benvinguda de IT ja conté instruccions adreçades al personal sobre la necessitat de no fer servir unitats de memòria o equips diferents dels previstos per l'organització.

És important assenyalar que l'àrea de treball en què es fa servir Linux resta fora de l'àmbit de control i actualització dels serveis informàtics centrals de l'organització.

Àrees de millora

●	Com a possible element de millora de la seguretat, seria necessari que l'àrea de Linux de l'organització també es trobés sota les mesures de seguretat i control que preveuen els serveis informàtics centrals de l'organització.

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 *in situ* durant la visita a les instal·lacions, l'entitat disposa de tres espais condicionats per a l'allotjament dels servidors: d'una banda, hi ha un CPD al cantó de muntanya i un altre al cantó de mar; d'altra banda, hi ha un tercer CPD que correspon a l'àrea on treballen amb Linux.

En totes les sales de servidors comprovem que s'hi apliquen les mesures de seguretat molt semblants. En tots els casos, l'accés està controlat per un sistema d'identificació per targeta, de manera que només el personal d'informàtica, manteniment i serveis generals hi tenen accés autoritzat. Les sales estan refrigerades, gràcies a diversos sistemes d'aire condicionat, i estan proveïdes de sistemes de detecció de fum i control de temperatura.

En el cas del CPD de muntanya també hi ha instal·lat un sistema que previndria i eliminaria possibles problemes de condensació d'aigua.

Cada armari destinat a servidor disposa del seu propi SAI, que permetria disposar d'un corrent elèctric alternatiu per al cas d'una improbable interrupció sobtada del corrent elèctric.

Només com elements de millora, caldria tenir en compte que no s'han pogut verificar l'existència d'extintor al CPD de mar i de sistema de detecció de fum a l'àrea de Linux. D'altra banda, és important tenir en compte que el CPD de l'àrea de Linux, per una qüestió particular de l'organització, resta forma del control dels serveis informàtics de l'organització, cosa que pot plantejar algun problema de seguretat.

L'accés a internet està controlat per un Firewall perimetral Juniper, que preveu el filtratge de totes les entrades i sortides de telecomunicacions per motius de seguretat.

Àrees de millora

●	Tot i que en general les sales de servidors estan dotades de mesures de seguretat adequades, caldria verificar l'existència d'un extintor a l'abast al CPD de mar i d'un sistema de detecció de fum al CPD de l'àrea de Linux. També seria necessari que les mesures de seguretat de l'àrea de Linux en general es trobessin sota el control dels recursos informàtics generals de l'organització.

5.13. EMMAGATZEMATGE DE FITXERS

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

Situació actual

El document de benvinguda d'IT que es proporciona al personal ja conté un seguit d'instruccions de seguretat en un apartat específic sobre bones pràctiques. En particular, s'hi fa constar una recomanació de no desar la informació al servidor local, sinó de fer servir sempre les eines, carpetes i recursos compartits. També s'hi determina una prohibició expressa de no fer servir dispositius extraïbles (pendrives o discs externs, entre d'altres) per al tractament de la informació sensible.

En general, els equips informàtics de l'entitat no duen els ports capats, però la prohibició expressa de fer servir unitats de memòria externa hauria de ser suficient per a desincentivar-ne qualsevol ús.

D'altra banda, es comprova durant els treballs de camp que el tractament de les dades personals es du a terme habitualment a l'entitat a través dels entorns informàtics previstos per l'entitat, que són el domini actiu, el correu electrònic i el software de gestió SAP, entre d'altres.

No consta que hi hagi tractaments de dades que es facin generalment fora dels sistemes i entorns informàtics previstos per l'entitat.

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*" i les informacions proporcionades, l'entitat té implementats diversos procediments de realització de còpies de seguretat, que apareixen en el document citat correctament documentats i descrits. Resumim aquí sota els quatre procediments descrits.

Freqüència de la còpia / Període de conservació / Suport utilitzat

- Diària / 1 mes / 1 mes / En un altre dispositiu (servidor)
- Setmanal / 4 setmanes / En un altre dispositiu (servidor)
- Anual / 5 anys / Cintes de memòria
- Mensual / 12 mesos / Cintes de memòria

D'acord amb el protocol i les informacions proporcionades, el software que fa les còpies ja inclou un control d'integritat, que s'aplica quan la còpia ha estat realitzada. D'altra banda, ja es fan revisions i proves de restauració de forma periòdica sobre els diferents els procediments de còpia i recuperació. Els elements a controlar responen a una selecció aleatòria.

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, d'entrada, ja ha dues unitats diferenciades que permeten distingir l'accés del personal d'administració del que correspon al personal investigador. D'altra banda, segons el document aportat a aquesta auditoria "*Política de seguridad de ficheros*", cada unitat d'administració o grup de recerca té la seva pròpia carpeta de grup amb permisos exclusius de lectura i escriptura per als membres del grup.

Per tot plegat, constatem que ja s'han definit diferents perfils d'accés sobre les dades i els permisos que pot tenir el personal a l'hora a l'hora de manipular-les o visualitzar-les.

A l'entitat es manté una relació dels usuaris que té clau i té un accés autoritzat a les instal·lacions. També estan registrats els usuaris que han de tenir accés a determinades restringides mitjançant targeta. Aquests registres es mantenen actualitzats, ja que hi ha procediments definits d'alta, modificació i baixa d'usuaris que permeten una comunicació entre l'àrea de recursos humans i els responsables informàtics. En general, aquesta comunicació es vehicula a través d'un full Excel.

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

En general, el procediment d'alta d'un nou usuari autoritzat de les dades s'acompanya sempre d'un procediment d'acollida en què es defineixen els recursos i accessos a què ha de tenir accés i se n'informa els responsables informàtics perquè ho apliquin. Aleshores, els responsables informàtics proporcionen per correu electrònic al responsable organitzatiu de l'àrea en què s'incorpora la nova persona el seu nom d'usuari i una contrasenya provisional, per tal que pugui accedir als entorns que correspongui. Durant el primer accés, la nova persona podrà canviar les contrasenyes provisionals per unes de noves, seguint uns criteris predefinits. De forma habitual, el nom d'usuari és la inicial del nom i el cognom.

En general, tots els entorns informàtics de l'entitat estan protegits per control de nom d'usuari i contrasenya. En particular, els procediments d'accés al domini actiu i al correu electrònic comparteixen uns mateixos criteris de robustesa en la definició de contrasenya que no tenen els accessos al NorayBanks i al SAP. No obstant, per a l'accés al SAP i al NorayBanks és necessari l'accés previ al domini de l'organització.

Les característiques de les contrasenyes que es fan servir per a l'accés al domini i al correu electrònic, d'acord amb les informacions proporcionades, han de tenir les següents característiques:

- Longitud mínima de 8 dígits.
- Ha de combinar majúscules, minúscules, dígits caràcters no alfanumèrics (com a mínim, ha de combinar caràcters de tres d'aquestes categories)
- No pot incloure part o la totalitat del nom de l'usuari.
- Manté un record històric que no permet que es repeteixin les 10 darreres contrasenyes.
- Cal renovar-les cada 180 dies.

D'altra banda, per a l'accés al domini s'apliquen mesures de limitació per intents d'accés fallit. En el cas de l'AEGERUS, es permeten fins a 3 intents d'accés, després dels quals es bloqueja l'accés.

També s'aplica a l'organització una mesura de bloqueig per inactivitat, que s'aplica al cap de 10 minuts d'inactivitat en qualsevol equip.

En el cas del correu electrònic, és important constatar també que s'apliquen sistemes de doble autenticació en relació al seu ús en nous dispositius, cosa que aporta una major seguretat addicional en la identificació i control de la persona usuària. A aquest efecte constitueix una evidència el document "*Configurar acceso multifactor*"

No detectada

▲	

5.17. ACCESSOS REMOTS

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

Situació actual

L'entitat permet a determinats usuaris, per raons justificades de les seves responsabilitats laborals, que accedeixin remotament als sistemes.

D'altra banda, com a conseqüència sobretot de la crisi sanitària provocada per la Covid-19 i la impossibilitat que els treballadors poguessin desplaçar-se al seu lloc de treball, s'ha concedit també accés remot a perfils professionals que no el tenien ni el necessitaven anteriorment.

L'accés remot ha d'estar autoritzat específicament per la direcció de l'entitat i implica connectar-se a través de VPN o d'un sistema d'accés a l'escriptori virtual. De forma prèvia, cal que l'entitat hagi instal·lat un software VPN a l'equip autoritzat per a l'accés remot. En tot cas, no és possible connectar-se de forma virtual sense passar per aquesta activació o instal·lació prèvia.

No consta que l'entitat hagi desenvolupat un protocol específic sobre teletreball, però sí que consten previsions i instruccions de seguretat sobre l'accés remot al document "*Condiciones de uso de la infraestructura informàtica*".

Recordem també que s'apliquen diferents mesures de seguretat en l'accés al sistema, com són el Firewall Juniper i l'antivirus Kaspersky. També s'hi aplica una mesura de bloqueig per inactivitat en l'accés al domini.

Per tot plegat, es minimitza notablement la possibilitat d'accessos indeguts des de fora de les instal·lacions i mitjançant dispositius o equips que escapin al control de l'entitat.

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 fa servir eines que li permeten dur a terme el registre i control dels accessos informàtics. D'una banda, un software anomenat LANSWEEPER permet auditar accessos als equips informàtics. D'altra banda, l'ús del software DATA SECURITY PLUS implica poder controlar els accessos al servidor d'arxius. D'aquesta manera, és possible revisar i comprovar quin usuari ha accedit i/o eliminat una carpeta determinada.

Encara que l'entitat demostri tenir les eines informàtiques necessàries 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.

En definitiva, si bé l'entitat pot obtenir la informació rellevant sobre els accessos, aquesta actuació es realitzaria de forma reactiva.

En qualsevol cas, resulta evident que l'entitat du a terme tractaments a gran escala de dades 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

●	És possible millorar la prevenció d'accessos indeguts mitjançant l'establiment d'un procediment de revisió d'accessos i intents d'accessos, que caldria documentar i definir. 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, tots els suports i dispositius que es fan servir a l'entitat per a tractar i conservar dades de caràcter personal ja estan degudament identificats i inventariats. Tots porten una etiqueta que els identifica i que permet relacionar-los amb la persona usuària a qui estan assignats.

Tal com hem comentat al punt anterior, l'entitat disposa d'una eina informàtica anomenada LANSWEEPER que permet identificar els diferents equips de l'entitat i relacionar-los amb l'usuari que tenen assignat. D'aquesta manera, és possible saber en tot moment a quina persona està assignada a un determinar dispositiu, suport o recurs informàtic.

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

No detectada

▲	

5.20. DESTRUCCIÓ DE SUPORTS

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

Situació actual

Pel que fa a la documentació en paper, constatem que l'entitat disposa de màquines trituradores i contenidors de destrucció segura a totes les àrees en què es fa servir documentació en paper de manera habitual, com per exemple a l'àrea de recursos humans, on hi ha dues màquines trituradores. Per a la gestió de la destrucció segura, l'entitat té contractada l'empresa especialitzada CESPA, que buida els contenidors de tan en tant i, després de destruir-ne el contingut, emet certificats de destrucció segura.

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 procediments que requereixen la conservació dels suports com a evidència.

Pel que fa a la destrucció de suports i dispositius informàtics que s'han fet servir per al tractament de les dades, primer de tot es constata que, d'acord amb les bones pràctiques que fomenta l'entitat, no haurien de contenir dades gravades localment. No obstant, també es fan servir en aquest cas els serveis d'una empresa de destrucció segura, que emet certificats de les accions de destrucció de suports i dispositius.

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.

Només en determinades àrees es detecta l'existència de procediments de comunicació de dades, els quals ja apliquen i tenen en compte mesures de seudonimització o procediments d'encriptació que impliquen l'ús del software Winzip. Així, per exemple, a l'àrea de serveis generals hi ha comunicacions amb l'hospital d'informació relativa a usuaris que impliquen que el document, quan s'envia per correu electrònic, vagi encriptat amb Winzip. En la gestió de les factures rebudes s'apliquen generalment procediments de seudonimització que impliquen no poder identificar les persones sobre les quals es demanen o generen informes. En el cas de les proves genètiques, els informes generats per l'entitat inclouen les sol·licituds i la identitats del client, però es justifica per una qüestió de qualitat procedimental.

Per tant, en definitiva, no consten, en termes generals, procediments d'enviament d'informació sensible per correu electrònic de forma sistemàtica, però sí alguns procediments localitzats en determinades àrees, que ja apliquen procediments d'encriptació, d'acord amb les informacions proporcionades. També es constata l'existència d'instruccions de seguretat que contemplen de forma específica com s'han de tractar les transferències de dades que continguin dades de categoria especial.

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 recursos humana, 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

D'acord amb les informacions proporcionades, la documentació en suport paper que es fa servir a l'entitat es troba generalment desada als seus corresponents armaris, situats en despatxos 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. No obstant, hi ha encara alguns arxius actius en diferents àrees de treball. En aquestes àrees, les úniques 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 del cap 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. Cal tenir en compte que la documentació relativa a estudis observacionals s'ha de conservar durant 15, mentre que la documentació relativa a assajos clínics requereix una conservació mínima de 25 anys. D'entrada, 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'entitat manifesta haver fet accions de destrucció de documentació antiga. Segons les informacions proporcionades, aquestes accions s'han fet amb la col·laboració d'una empresa de gestió i destrucció documental, que ha emès els corresponents certificats de destrucció segura.

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 RRHH: En armaris tancats amb clau, es guarden els expedients del personal, sota la custòdia de les persones responsables de recursos humans. La documentació es guarda generalment seudonimitzada, i no es guarda només per al manteniment de la relació laboral, sinó també per a servir d'evidència en l'acreditació dels projectes. Quan un treballador és baixa definitiva, la seva carpeta es trasllada a l'arxiu passiu, on es continuarà conservant seudonimitzada de manera indefinida, per tal de continuar servint com a evidència del personal involucrat als projectes. 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 administratiu o financer: En determinats espais on es du a terme la gestió econòmic-financera de l'organització es mantenen desats contractes i convenis que l'entitat ha signat, desats en armaris tancat amb clau, sota la responsabilitat del responsable de l'àrea. A banda d'aquests contractes, en la gestió ordinària de la facturació o de la gestió econòmica no es genera avui dia cap altre tipus de documentació.

Arxius actiu de recerca: Els expedients dels projectes de recerca actiu es troben custodiats pels corresponents investigadors, que els mantenen desats en armaris tancats amb clau. Només els investigadors adscrits a cada projecte poden accedir a la documentació corresponent. Un cop el projecte deixa d'estar actiu, la documentació es trasllada a l'arxiu passiu.

Arxiu passiu general: Es troba en un espai annex a l'hospital, proveït de sistemes de tancament i només accessible per al personal responsable de l'arxiu (a banda de personal de manteniment i seguretat), que depèn de l'àrea de serveis generals. Aquí s'hi guarden 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 els 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.

En general, la documentació es conserva generalment de manera indefinida.

Àrees de millora

●	D'acord amb els principis de conservació de les dades i davant la possibilitat que es guardin dades més enllà del que seria necessari i justificat, 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 de tractament. 5.3. Definició de les mesures de seguretat per part del responsable del tractament. 5.4. Delegat de protecció de dades. 5.5. Encarregats del tractament i proveïdors sense accés a dades. 5.6. Licitud del tractament, base jurídica, informació i consentiment. 5.8. Notificacions de violacions de seguretat. 5.9. Difusió de funcions i obligacions del personal.
II – BLOC DE MESURES DE SEGURETAT
5.11. Manteniment de les xarxes. 5.12. Centre de processament de dades. 5.18. Registre d'accessos informàtics. 5.24. Criteris d'arxiu.

Barcelona, 25 de juliol de 2021.

Pere Ruiz Espinós

- Soci -

Caterina Bartrons Pou

- Gerent -