

	Informe d'Auditoria RGPD
Delegada de Protecció de dades: Iris Bargalló	Data: 18/12/2020

Taula de Contingut

1	Introducció	2
2	Objectiu	2
3	Responsabilitats	2
4	Metodologia	2
5	Unitats Auditades	3
6	Descripció de l'Activitat	3
7	Auditoria	4
7.1	Realització	4
7.2	Punts forts	4
7.3	Àrees de Millora.....	4
8	Resultats i No Conformitats	4
8.1	Amics de Can Ruti.....	4
8.2	Finances	5
8.3	Compres	5
8.4	Secretaria Direcció	6
8.5	IT.....	6
8.6	Comunicació	7
8.7	Secretaria Direcció	7
8.8	Serveis Generals.....	7
8.9	Lab Managing.....	7
8.10	Plataformes	8
8.11	Grant Management.....	8
8.12	Legal	8
8.13	Biobanc.....	8
8.14	Neurogenètica	9
8.15	REMAR.....	9
8.16	UPIC	10

8.17	ITO.....	10
8.18	GCAT	10
8.19	Grup d'Investigació de Virologia Clínica i Noves Aproximacions Diagnòstiques.....	11
8.20	CMCiB	11
8.21	Programa de Medicina Predictiva i Personalitzada del Càncer (PMPPC).....	11
8.22	HHRR	12
8.23	Grup d'Investigació de malalties infeccioses Respiratòries i Tuberculosis... ¡Error! Marcador no definido.	
8.24	Terminis d'implantació	12
9	Avaluació, manteniment i avaluació de les pràctiques de protecció de dades.....	12
10	Referències	12
11	Annexa	13
12	Aprovació	13

1 Introducció

Durant el 2018-2019, l'IGTP ha implementat les mesures de protecció de dades necessàries per complir amb el nou Reglament general de protecció de dades (RGPD 2016/679) i la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

En el període de Setembre 2019- Desembre 2020 s'han realitzat auditories internes per tal d'evidenciar el compliment i la adaptació de les accions correctores identificades durant el període d'implementació. El període d'auditories s'ha vist afectat per la pandèmia i s'ha hagut d'estendre en el temps per tal de poder fer les visites in situ.

2 Objectiu

L'objectiu d'aquest informe és identificar les àrees que s'han de resoldre i les accions que s'haurà de dur a terme per corregir les no conformitats detectades durant l'auditoria interna i adaptar-se als requeriments del reglament i llei esmentats anteriorment.

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.

3 Responsabilitats

Gerent – Sr. Carles Esquerrè

Delegada de Protecció de dades – Sra. Iris Bargalló

4 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.

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 en el pla d'auditoria presentat al Setembre 2019, 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

L'auditoria interna de dades personals s'ha realitzat per a tots els unitats de l'IGTP indicades en el punt següent amb la col·laboració i l'aprovació de tots els representants de les unitats. Les no conformitats identificades en cada exercici ha quedat documentat i s'ha facilitat una còpia a cada unitat corresponent.

5 Unitats Auditades

Els següents unitats han participat en l'auditoria interna de dades personals:

- Amics de Can Ruti (Anna Duran)
- Finances (Silvia Andrade, Àngels Serra i Paula Amarin)
- Compres (Judit Capitán)
- Secretaria de Direcció (Meritxell Nevado)
- IT
- Biobank
- CEIC
- CMCiB
- Compres
- Comunicació
- Diagnòstic Genètic
- Finances
- GCAT
- Grant Management
- Grups de Recerca
- HHRR
- Innovation & Transfer Office
- Lab Managing
- Secretaria Direcció
- Serveis Generals
- UPIC
- Plataformes

6 Descripció de l'Activitat

L'Institut de Recerca Germans Trias i Pujol (IGTP) és un centre de recerca públic situat a Badalona (Barcelonès) que té com a objectiu principal incrementar el coneixement científic per transformar-lo a continuació en una millor salut i atenció mèdica dels pacients i de la comunitat.

La Missió de l'IGTP és crear un entorn multi-disciplinar i multi-institucional que permeti fer recerca translacional amb la màxima eficiència per millorar la salut i la qualitat de vida de les persones.

7 Auditoria

Després de l'avaluació de la preparació, s'ha desenvolupat i definit un pla d'acció per corregir les no conformitats identificades durant les auditories de dades personals. Aquests s'han prioritzat tenint en compte els riscos implicats per a la persona interessada i la institució, equilibrats amb el nivell d'esforç i recursos necessaris.

Les no conformitats i el pla d'acció complet estan llistats, definits i prioritzats en el document "Informe No Conformitats Auditoria RGPD i pla CAPA de IGTP"

El pla serà aprovat per Direcció i inclourà accions per a cada unitat.

7.1 Realització

Les auditories s'han realitzat en bon ambient amb la col·laboració de tot els equips del IGTP. Durant els dos dies es va entrevistar els membres del personal de les unitats abans esmentades i tots van estar oberts i disposats a respondre a totes les consultes i proporcionar la màxima informació possible.

7.2 Punts forts

Durant l'auditoria s'ha pogut evidenciar que el personal de l'IGTP està ben format per realitzar el seu treball i és coneixedor dels requisits del RGPD i de com protegir les dades personals.

Totes les dades personals a nivell d'oficina estan ben protegides electrònicament mitjançant diferents permisos d'accés a les diferents àrees de treball amb carpetes compartides entre els departaments, on els empleats només poden accedir a la informació i dades rellevants per a la realització de la seva feina.

Disposen de una sala de servidors amb control d'entrada, es fan còpies de seguretat periòdicament i la informació sensible es guardada en armaris amb clau.

Les instal·lacions del IGTP estan dividides en tres edificis, Mar, Muntanya, i CMCiB els quals tenen control d'accés físic mitjançant una targeta d'accés i personal de seguretat a l'entrada. Els despatxos de les diferents Unitats també disposen de clau.

7.3 Àrees de Millora

Problemes en els fluxes d'informació que arriben als investigadors alguns no saben de l'existència de models d'acords MTA i DTA. Tampoc els hi ha arribat informació sobre les xerrades de protecció de dades, codi de conducta o vídeo d'introducció al RGPD.

Alguns investigadors treballen amb ordinadors personals el que implica un risc ja que no es garanteixen les mesures de seguretat institucionals.

Es fan servir plataformes no institucionals com Dropbox, GDrive.

8 Resultats i No Conformitats

Seguint els resultats de les auditories de cada unitat, s'indica a continuació les principals no conformitats identificades com a risc potencial per a les persones i l'IGTP.

8.1 Amics de Can Ruti

8.1.1 Data d'auditoria: 20/09/19

8.1.2 Persones entrevistades: Anna Duran i Silvia Andrade

8.1.3 No Conformitats:

1. **Dades personals en ordinador personal:** Anna Duran té les dades personals de donants en el seu ordinador personal. L'ordinador no té implementades les mesures de seguretat de l'IGTP.

Acció Correctora: Es recomana que es faciliti un ordinador portàtil d'empresa.

2. **Emails amb arxius que contenen dades personals:** S'envien emails a Finances regularment amb arxius que contenen dades personals sense contrasenya.

Acció Correctora: Es recomana que es generi una carpeta compartida entre Anna Duran i Finances.

8.1.4 Recomanacions:

1. **Certificats de donació:** Els donants que sol·liciten el certificat, envien les dades per correu.

Acció Correctora: Es recomana que es generi un formulari on els sol·licitants puguin completar les dades directament i que bolqui la informació a un Excel.

8.2 Finances

8.2.1 Data d'auditoria: 20/09/19

8.2.2 Persones entrevistades: Silvia Andrade, Àngels Serra i Paula Amorin.

8.2.3 No Conformitats:

1. **Finances rep informació identificativa dels pacients** sense codificar o pseudonimitzar de Neurogenètica i les proves diagnòstiques que han realitzat. Aquest tipus de dades estan considerades com a categories especials de dades, segons el RGPD necessàriament s'ha de tenir una base legal específica per al seu tractament.

Acció Correctora: Sensibilitzar als hospitals sol·licitant.

2. **Participants en assajos clínics, es té informació de l'assaig en què estan participant.** Aquest tipus de dades està considerat com a categories especials de dades, segons el RGPD necessiten un licitud específica per al seu tractament, que el unitat de finances no té. Els laboratoris son els que demanen el nom de l'assaig per poder facturar
En la factura del promotor nomes surt el nom assaig amb codi de pacient, a l'abonament surt el nom del pacient i el codi de l'assaig. Existeix una separació funcional entre el personal que gestiona la factura i l'abonament, però ambdues tenen accés a les carpetes, per el que es possible vincular a la persona amb l'assaig.

Acció Correctora: Es recomana implementar una separació tècnica impedit que qui gestioni la factura no pugui accedir a l'abonament i a l'invés.

8.3 Compres

8.3.1 Data d'auditoria: 20/09/19

8.3.2 Persones Entrevistades: Judit Capitán

8.3.3 No Conformitats: No Detectades

8.4 Secretaria Direcció

8.4.1 Data d'auditoria: 20/09/19

8.4.2 Persones Entrevistades: Meritxell Nevado

8.4.3 No Conformitats: No Detectades **Falta revisar la part que gestiona l'Esther Casafont.**

8.5 IT

8.5.1 Data d'auditoria: 11/10/19

8.5.2 Persones entrevistades: Ruben Cobos, José Ponce, Sergio Tamayo, Tadeo Lava

8.5.3 No Conformitats:

3. **Servidors amb dades mèdiques per a recerca no disposa d'auditoria d'arxius:** Els servidor on es guarden les dades mèdiques per a recerca no disposa de registre d'accessos ni d'accions.

Acció Correctora: S'ha d'integrar auditoria d'arxius per accés i modificació en servidors o plataformes on es guardin dades mèdiques.

4. **Correus amb arxius que contenen dades personals:** S'envien emails des de Gestió de Personal regularment amb arxius que contenen dades personals sense contrasenya.

Acció Correctora: Es recomana que es generi una carpeta compartida entre IT, SSGG, Gestió de Personal i Lab Managing.

5. **No es comuniquen a IT les baixes de personal:** El que comporta que persones que ja no treballen a la institució puguin tindre accés a comptes de correu i àrees de treball.

Acció Correctora: S'han de comunicar les baixes de personal a IT.

8.5.4 Recomanacions:

1. **Manual de Seguretat TIC:** Es recomana que es generi un manual de seguretat on indiqui:
 - Infraestructures i sistemes
 - Enllaços a Internet i Firewall
 - Antivirus
 - Núvol Local i/o Privat
 - Plataforma correu
 - Altres plataformes
 - Seguretat física
 - Seguretat Lògica
 - Seguretat de Dades
 - Gestió i Controls d'Usuaris
 - Gestió de Documents
 - Destrucció
 - Redundàncies i Rèpliques de màquines virtuals (si aplica)
 - Còpies de Seguretat
 - Pla de Contingència

8.6 Comunicació

8.6.1 Data d'auditoria: 11/10/2019

8.6.2 Persones entrevistades: Roser Montserrat, Harvey Evans.

8.6.3 No Conformitats: No es detecten no conformitats.

8.6.4 Recomanacions:

1. Formularis en Typeforms: es recomana afegir un link a la política de privadesa del IGTP.
<http://www.germanstrias.org/es-legal-notice/>

8.7 Secretaria Direcció

8.7.1 Data d'auditoria: 11/10/19

8.7.2 Persones Entrevistades: Ester Casafont

8.7.3 No Conformitats: No Detectades

8.8 Serveis Generals

8.8.1 Data d'auditoria: 11/10/19

8.8.2 Persones entrevistades: Quim Puig

8.8.3 No Conformitats:

1. Emails amb arxius que contenen dades personals: S'envien emails des de Gestió de Personal regularment amb arxius que contenen dades personals sense contrasenya.

Acció Correctora: Es recomana que es generi una carpeta compartida entre IT, SSGG, Gestió de Personal i Lab Managing.

2. No es comuniquen a SSGG les baixes de personal: El que comporta que persones que ja no treballen a la institució puguin tindre accés a l'edifici i a diferent àrees de treball.

Acció Correctora: S'han de comunicar les baixes de personal a SSGG.

8.9 Lab Managing

8.9.1 Data d'auditoria: 08/11/19

8.9.2 Persones entrevistades: Natalia Ruiz, David Izquierdo

8.9.3 No Conformitats:

3. Emails amb arxius que contenen dades personals: S'envien emails des de Gestió de Personal regularment amb arxius que contenen dades personals sense contrasenya.

Acció Correctora: Es recomana que es generi una carpeta compartida entre IT, SSGG, Gestió de Personal i Lab Managing.

4. **No es comuniquen a Lab Managing les baixes de personal:** El que comporta que persones que ja no treballen a la institució puguin tindre accés a l'edifici i a diferent àrees de treball restringides

Acció Correctora: S'han de comunicar les baixes de personal a Lab Managing.

5. **Mostres amb informació pseudonimitzada es poden quedar a recepció de l'edifici sense control en cas que la persona de recepció no estigui en aquell moment:** El que comporta un risc d'accés il·lícit a les dades o a la integritat d'aquestes mostres.

Acció Correctora: Es recomana que les mostres s'entreguin al receptor/a directament en comptes de en recepció.

8.10 Plataformes

8.10.1 Data d'auditoria: 08/11/19

8.10.2 Persones entrevistades: Marco Fernández, Maria del Pilar Armengol Barnils y Jose Maria Hernandez Perez

8.10.3 No Conformitats: No Detectades

8.10.4 Recomanacions: En el departament de Genòmica transaccional, l'informe dels resultats de les proves sol·licitades per el departament de Immunologia s'entreguen en mà, tot i que no es una no conformitat i el sistema es segur, per tal d'agilitzar i facilitar el procés es recomana la creació d'una carpeta compartida per agilitzar el procés d'entrega

8.11 Grant Management

8.11.1 Data d'auditoria: 08/11/19

8.11.2 Persones Entrevistades: Oscar Fraile

8.11.3 No Conformitats: No Detectades

8.12 Legal

8.12.1 Data d'auditoria: 08/11/19

8.12.2 Persones Entrevistades: Janire Gesto

8.12.3 No Conformitats: No Detectades

8.12.4 Recomanacions: Tot i que no es tracten dades personals, en el departament es gestiona informació confidencial, per el que es recomana la creació d'una carpeta pròpia on només tingui accés Janire Gesto.

8.13 Biobanc

8.13.1 Data d'auditoria: 29/11/19

8.13.2 Persones entrevistades: Natal Edurne Pedrosa, Laia Pérez

8.13.3 Recomanacions:

6. **Mostres amb nom i cognoms de pacients en Biobanc sòlid:** Les mostres, en general, estan codificades però les mostres anteriors al 2017 tenen nom i cognom. Les mostres estan localitzades al departament on només té accés anatomia patològica.

Acció Correctora: Es recomana la codificació de totes les mostres i evitar l'ús de nom del pacient, especialment a les mostres que no pertanyen al HUGTP.

7. **Zones de Congeladors no restringida en Biobanc IGTP:** l'accés a l'edifici es restringit, però no la zona dels congeladors on es troben totes les mostres.

Acció Correctora: Es recomana implementar control d'accés a la zona dels congeladors de l'Edifici Mar.

8.13.4 No Conformitats:

1. **Anatomia del HUGTP té accés a les mostres del IGTP per a serveis a tercers:** El que comporta que persones del HUGTP puguin tindre accés a informació de mostres que tercers han sol·licitat al IGTP.

Acció Correctora: Creació de carpeta restringida al HUGTP per a l'equip del Biobanc sòlid del IGTP.

2. **Zones de Congeladors no restringida en Biobanc sòlid:** l'accés a un dels congeladors es de lliure accés dins l'HUGTP. L'altre es troba tancat en una "gàbia" amb clau.

Acció Correctora: Es recomana instal·lar el congelador que està en la zona de lliure accés a la "gàbia" on es troba el segon congelador ja que està tancada amb clau i només el personal del Biobanc en té accés.

8.14 Neurogenètica

8.14.1 Data d'auditoria: 29/11/19

8.14.2 Persones entrevistades: Dr. Antoni Matilla

8.14.3 No Conformitats:

1. **Finances rep informació identificativa dels pacients sense codificar o pseudonimitzar de Neurogenètica i les proves diagnòstiques que han realitzat.** Aquest tipus de dades estan considerades com a categories especials de dades, segons el RGPD necessàriament s'ha de tenir una base legal específica per al seu tractament, aplicar mesures de seguretat i accés restringit.

Acció Correctora 1: Creació de carpeta compartida Neurogenètica/Finances i establir un procediment on la documentació escanejada s'envii directament a la carpeta compartida amb Finances o bé enviar la documentació protegida amb contrasenya.

Acció Correctora 2: Sensibilitzar als hospitals sol·licitants per a que no enviïn les sol·licituds de probes amb nom de pacient.

8.15 REMAR

8.15.1 Data d'auditoria: 10/01/20

8.15.2 Persones entrevistades: Miriam Morón Font, Núria Pujol Furelos, Sergio Arté Garcia, aura Carreras Planella, Francesc Borràs Serres, Marcel.la Franquesa Bartolomé

8.15.3 Recomanacions:

6. [La majoria dels integrants del departament no tenen ordinador de la institució i treballen en ordinadors personals](#). Els ordinadors personals no tenen implementades les mesures de seguretat de l'IGTP.

[Acció Correctora](#): Es recomana que es faciliti un ordinador portàtil d'empresa.

7. [Suports de paper amb dades personals guardats a armaris sense clau](#).

[Acció Correctora](#): Es recomana que es guardin en armaris amb clau.

8.15.4 No Conformitats:

1. [Zones de Congeladors no restringida](#): l'accés a l'edifici es restringit, però no la zona dels congeladors on es troben totes les mostres.

[Acció Correctora](#): Es recomana implementar control d'accés a la zona dels congeladors de l'Edifici Mar.

8.16 UPIC

8.16.1 Data d'auditoria: 22/02/20

8.16.2 Persones entrevistades: Dra. Barriocanal, Dr. Magin

8.16.3 Recomanacions:

8. [Accés a l'arxiu de la unitat obert durant horari laboral](#).

[Acció Correctora](#): Es recomana que es tanqui amb clau encara que hi hagi personal a la unitat.

8.16.4 No Conformitats:

1. [No Detectades](#)

8.17 ITO

8.17.1 Data d'auditoria: 22/02/20

8.17.2 Persones entrevistades: [Marc Cusachs Farraro](#)

8.17.3 No Conformitats:

1. [No Detectades](#)

8.18 GCAT

8.18.1 Data d'auditoria: 06/03/20

8.18.2 Persones entrevistades: Dr. Rafael de Cid

8.18.3 No Conformitats:

2. [No Detectades](#)

8.19 Grup d'Investigació de Virologia Clínica i Noves Aproximacions Diagnòstiques8.19.1 Data d'auditoria: 06/03/208.19.2 Persones entrevistades: Dra. Elisa Martos8.19.3 No Conformitats:

9. [Falten acords de tractaments de dades amb institucions amb les que es col·labora i amb les que es dona serveis.](#)

[Acció Correctora:](#) Revisió de tots els contractes amb tercers on hi hagi intercanvi de mostres i/o dades personals.

8.20 CMCiB8.20.1 Data d'auditoria: 27/11/20208.20.2 Persones entrevistades: Sara Capdevila, Patricia Fachal.8.20.3 No Conformitats:

1. [No Detectades](#)

8.20.4 Observacions:

1. [Plataformes Actuals:](#) S'hauria de revisar els contractes de les plataformes AniBio i DiTec per garantir que els acords inclouen les condicions per al tractament de dades
2. [Plataforma QUIBIN:](#) Realitzar Avaluació de Seguretat i Avaluació D'Impacte de Protecció de Dades- El dia 17/12/20 es faciliten les plantilles
3. [Web CMCiB:](#) La web no té política de privacitat, es recomana afegir-ne una en relació a com es tractaran les dades personals dels pacients.

8.21 Programa de Medicina Predictiva i Personalitzada del Càncer (PMPPC)8.21.1 Data d'auditoria: 27/11/20208.21.2 Persones entrevistades: Miguel Ángel Peinado, Berta Martín Abad, Mar Muñoz Mata8.21.3 No Conformitats:

1. [Problemes en els fluxes d'informació que arriben als investigadors](#)
 - a. [No saben de l'existència de models d'acords MTA i DTA](#)
 - b. [No els hi ha arribat informació sobre les xerrades de protecció de dades, codi de conducta o vídeo d'introducció al RGPD.](#)

[Acció Correctora:](#) Campanya de comunicació cap als investigadors on se'ls hi proporcioni la informació i formació en relació a protecció e dades.

2. [Ús d'ordinadors propis: no es pot garantir la seguretat de les dades de l'IGTP](#)

Acció Correctora: Proporcionar ordinadors de la institució a tots els empleats del IGTP o garantir la implementació i manteniment d'ordinadors personals.

8.22 HHRR

8.22.1 Data d'auditoria: 03/12/2020

8.22.2 Persones entrevistades: Montse González

8.22.3 No Conformitats:

3. **No Detectades, les detectades en la primera visita d'avaluació s'han solventat.**

8.23 Grup d'Investigació en Innovació en Infeccions Respiratòries i Tuberculosis

8.23.1 Data d'auditoria: 04/12/2020

8.23.2 Persones entrevistades: José Antonio Domínguez Benítez, Raquel Villar Hernández

8.23.3 No Conformitats:

10. **Problemes en els fluxes d'informació que arriben als investigadors**
 - a. **No els hi ha arribat informació sobre les xerrades de protecció de dades, codi de conducta o vídeo d'introducció al RGPD.**

Acció Correctora: Campanya de comunicació cap als investigadors on se'ls hi proporcioni la informació i formació en relació a protecció de dades.

11. **Ús d'ordinadors propis: no es pot garantir la seguretat de les dades de l'IGTP**

Acció Correctora: Proporcionar ordinadors de la institució a tots els empleats del IGTP o garantir la implementació i manteniment d'ordinadors personals.

12. **Documentació amb dades personals guardada en armaris sense clau al laboratori**

Acció Correctora: Facilitar armaris amb clau.

8.24 Terminis d'implantació

Els terminis i les persones responsables assignades per mitigar i prevenir els riscos identificats durant l'exercici d'avaluació de protecció de dades s'han detallat a l'Informe Informe CAPA RGPD de IGTP. No obstant això, el termini objectiu per implementar totes les accions correctives és el 1/05/2021.

9 Avaluació, manteniment i avaluació de les pràctiques de protecció de dades.

Per satisfer contínuament el RGPD, L'IGTP farà un seguiment i documentaran evidència del compliment del RGPD mitjançant la creació d'un Pla d'auditoria de protecció de dades, que s'haurà de seguir i utilitzarà per recollir els resultats d'auditoria i establirà les bases per a un pla continu de millora de la protecció de dades.

10 Referències

- REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU 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)

- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals
- Registre d'Activitats de Tractament IGTP

11 Annexa

1. Informe CAPA RGPD de IGTP

12 Aprovació

Aquest pla d'acció RGPD ha estat aprovat i signat per el Sr. Carles Esquerrè, Gerent de l'IGTP.

Signatura:

Data:

.....

.....