FUNDACIÓ INSTITUT GUTTMANN

INFORME D'AUDITORIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Número de Protocol 10.951

ÍNDEX

1. Objectius i contingut

De conformitat amb el que estableix la normativa vigent sobre protecció de dades[1], tots els responsables de fitxer i/o encarregats de tractament que disposin de fitxers automatitzats i no automatitzats que continguin dades de nivell mitjà i/o alt, hauran de sotmetre, de forma biennal, els seus sistemes d'informació i instal·lacions de tractament de dades a una auditoria.

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.

[1] *Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (publicada en el BOE número 298, de 14 de desembre de 1999).*

Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (publicat en el BOE número 17, de 19 de gener de 2008).

Codi tipus de la Unió Catalana d'Hospitals.

2. Metodologia

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

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

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

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

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

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

3. Dades de l'entitat i treballs efectuats

3.1. Dades identificatives.

3.1.1. Dades entitat

Entitat	FUNDACIÓ INSTITUT GUTTMANN
NIF	G08519100
Domicili	Camí de Can Ruti s/n 08916 Badalona

3.1.2. Descripció de l'activitat

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

En data de 18 de juny de 2014 s'aprovà la fusió per absorció de la FUNDACIÓ PRIVADA INSTITUT DE NEUROREHABILITACIÓ GUTTMANN per la FUNDACIÓ INSTITUT GUTTMANN, la qual va tenir lloc l'1 de gener de 2015. Com a conseqüència d'aquesta fusió, totes les activitats dutes a terme per la FUNDACIÓ PRIVADA INSTITUT DE NEUROREHABILITACIÓ GUTTMANN passen a integrar-se dins les activitats de la FUNDACIÓ INSTITUT GUTTMANN, subrogant-se doncs en tots els drets i obligacions de l'entitat fusionada i extingida. Els serveis prestats per l'Entitat són els d'hospitalització d'aguts, d'Hospital de Dia, neurorehabilitació, consultes externes i recerca.

Les instal·lacions actuals de FUNDACIÓ INSTITUT GUTTMANN a Badalona són de 2002. D'altra banda, està impulsant un nou projecte (Guttmann Barcelona) als carrers Meridiana/Garcilaso de Barcelona, amb noves instal·lacions, que inclouran un gimnàs, sales de tractament, consultes mèdiques (Barcelona Health Institut) i 40 apartaments domotitzats per a persones amb necessitats especials (Guttmann Barcelona Life).

3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els diversos serveis i àrees de la Fundació Institut Guttmann:

- Delegat de Protecció de Dades

- Informàtica
- Recursos Humans
- Àrea de Docència
- Neuropsicologia (perfil)
- Responsabilitat Social i Corporativa i Comunicacions
- Admissions i Atenció a l'usuari i Arxiu
- Responsable de Seguretat de l'arxiu Neuropersonaltrainer
- Infermeria (perfil)
- Rehabilitació Funcional (perfil)
- Metge (perfil)
- Investigació / Recerca
- Àrea Econòmico-Financera

3.2.1. Data de realització de l'auditoria

Dies	24 i 25 de maig de 2018.

3.2.2. Persones entrevistades i relació de la documentació lliurada a l'auditor

Persones entrevistades per ordre d'intervenció:

NÚMERO	PERSONA ENTREVISTADA	ÀREA DE TREBALL
1	Sr. Javier Remacha	Delegat de Protecció de Dades
2	Sra. Cristina Vidal Sr. Pepe Pérez	Sistemes d'Informació
3	Sra. Elisenda Bassas	Recursos Humans
4	Sra. Mercès Solans	Àrea de Docència i Formació
5	Dra. Rocío Sánchez-Carrión	Neuropsicologia (perfil)
6	Sra. Elisabet González	RSC i Comunicacions
7	Sra. Elena Araujo	Admissions i Atenció a l'Usuari i Responsable d'Arxiu
8	Sr. David Hurtado	Responsable de Seguretat de l'arxiu NeuroPersonalTrainer
9	Sra. Àngels Barahona	Infermeria (perfil)
10	Sr. Ignasi Soriano	Rehabilitació Funcional (perfil)
11	Dra. Rosa Terré	Metge (perfil)
12	Dr. Josep M. Tormos	Investigació / Recerca

	Sr. Javier Solana Dr. Eloy Opisso	
13	Sra. Maria Esteve Sr. Hèctor López	Àrea Econòmico-Financera

Relació de la documentació i informació lliurada a l'auditor:

Document
Objecte social i Estatuts (article 7 dels Estatuts de l'entitat)
Organigrama dels departaments (a la web de l'entitat)
Codis d'inscripció dels fitxers inscrits a l'Agència Espanyola de Protecció de Dades
Document de Seguretat i Annexes
Esquema de la xarxa informàtica i de les bases de dades
Protocols interns de gestió: configuració d'internet i anella científica.
Documents d'informació i compromís professional
Documents del personal i consentiment de pacients
Contractes d'encarregat de tractament
Models de control dels registres establerts i llistats
Informes de revisió dels registres
Models per a l'exercici de drets d'accés, rectificació i cancel·lació i casos d'exercici
Informe de les auditories previstes en el reglament de mesures de seguretat
Elevació i aprovació de les conclusions de la darrera auditoria realitzada
Informes d'auditories i/o recomanacions rebuts dels auditors o dels assessors en protecció de dades. Resultat del control de qualitat del Codi tipus i documents sobre les mesures correctores que es van emprendre
Nomenament i inscripció del Delegat de Protecció de Dades
Registre d'Activitats de Tractament

Recol·lecció de les dades:

- ✓ Relació dels fitxers, estructura i contingut

- ✓ Polítiques de seguretat i procediments (registre d'incidències, còpies de seguretat, identificació i autorització, esborrat de suports, xifrat, etc.)
- ✓ Document/s de Seguretat
- ✓ Auditories anteriors
- ✓ Disseny físic i lògic dels sistemes d'informació
- ✓ Relació d'usuaris, accessos autoritzats i funcions
- ✓ Inventari de suports i registre d'entrada i sortida de suports
- ✓ Registre d'accessos i informes de revisió dels mateixos
- ✓ Etc.

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 salvetat 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.
	*Salvetat*, 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: Articles 96 i 110 RD 1720/2007.

Situació actual

La Fundació Institut Guttmann, en endavant l 'Entitat, va realitzar la darrera auditoria en matèria de protecció de dades el mes de juliol de 2016, complint d'aquesta manera amb les previsions legalment establertes per la legislació en protecció de dades.

Des de l'Entitat comenten que l'informe de l'auditoria de 2016 va ser elevat al Comitè de Direcció en la seva reunió de setembre 2016 (com es pot consultar l'acta a Gerència). També es va incloure la superació de l'auditoria 2016 en la Memòria d'Activitat 2016 aprovada pel Patronat FIG en la reunió de 22.6.2017 i en la Memòria-Balanç Social Informe de RSC pública (pàgina 2).

Des de l'Entitat s'aporta el Pla d'Accions Audit LOPD 2016, en què es recullen les mesures a adoptar a partir de les conclusions de la darrera auditoria.

Àrea de Millora

▲	No detectada	

5.2. Aspectes generals.

Base legal: Articles 79, 80 i 81 RD 1720/2007.

Situació actual

L'entitat ha fet entrega de les cartes de l'Agència Espanyola de Protecció de Dades (en endavant AEPD) amb els codis dels fitxers.

FITXER	CODI	FINALITAT	NIVELL	TRACTAMENT
Administració	2021970580	Realització dels processos habituals d'administració i comptabilitat	Bàsic	Parcialment automatitzat
Pacients	2021970576	Atenció assistencial, preventiva i rehabilitadora als pacients. Investigació, docència i planificació	Alt	Parcialment automatitzat
Personal	2021970583	Realització dels processos habituals de gestió de recursos humans i pagament de nòmines	Alt	Parcialment automatitzat
Reclamacions	2052770404	Garantir el dret a reclamar i a formular suggerències a l'Entitat per part dels ciutadans	Alt	Parcialment automatitzat
Externs	2103181151	Gestió de comunicació de l'Entitat de cara a l'exterior, gestió de voluntariat i personal col·laborador assistencial, empreses i col·laboradors externs, gestió dels amics de la Fundació, gestió d'alumnes Postgrau i altres.	Mig	Parcialment automatitzat
Guttmann NeuroPersonal Trainer	2131440039	Conté les dades dels professionals i pacients que utilitzen el programa Guttmann Neuropersonal Trainer, sent la finalitat donar seguiment a la prestació assistencial	Alt	Automatitzat
Investigació	2121180583	Gestió de les dades necessàries per la investigació, investigació	Alt	Parcialment automatitzat

		epidemiològica i activitats anàlogues, fins estadístics, històrics o científics.		
Videovigilància	2091030831	Videovigilància i control d'accessos a les instal·lacions	Bàsic	Automatitzat
Barcelona Brain Health Initiative	2171421800	Registre de les dades personals dels participants al projecte.	Alt	Parcialment automatitzat
Prevenció de blanqueig de capitals	2172131463	Prevenir o impedir operacions relacionades amb el blanqueig de capitals o el finançament del terrorisme	Alt	Parcialment automatitzat

Àrea de millora

🟠	Àrea de Millora	Caldria valorar si els Amics de l'Institut Guttmann hauria de ser un fitxer o tractament diferenciat dels "Externs", ja que la finalitat i naturalesa d'aquest tractament difereix del dels col·laboradors o estudiants que presten els seus serveis a l'Entitat. Recomanem que es consideri un tractament de dades diferenciat. Caldria valorar també si els participants del Sports & Life Guttman Club han de continuar classificats com a "Externs", quan els interessats provenen de participar en activitats de lleure organitzades per l'Entitat i no tenen res a veure amb el personal extern. Recomanem que es consideri igualment un tractament de dades diferenciat. **Observació d'acord amb el nou RGPD**: D'acord amb la nova legislació, la declaració dels fitxers no serà necessària, però, no obstant això, aquests es converteixen en Activitats de Tractament, les quals s'han de transcriure en un registre d'acord amb l'article 30 del RGPD. Es considera necessari tenir correctament regulats els fitxers per a l'efectiu trasllat com a activitat de tractament.

5.3. Document de seguretat.

Base legal: Articles 88, 95, 105 i 109 RD 1720/2007.

Situació actual

Mesures de seguretat
A. Existeix un document de seguretat (DS) per cada fitxer declarat o, per contra, es tracta d'un únic document de seguretat que inclou tots els fitxers declarats per l'entitat amb les especificitats pròpies de cadascun d'ells.
Comentaris: • L'Entitat ha elaborat un DS per cada un dels fitxers que té declarats en front l'AEPD, això és: o DS del Fitxer de Pacients o DS del Fitxer de Personal o DS del Fitxer d'Investigació o DS del Fitxer de GNPT o DS de Fitxer de Reclamacions o DS del Fitxer d'Externs o DS del Fitxer d'Administració o DS del Fitxer de Videovigilància o DS del Fitxer de Barcelona Brain Health Initiative o DS del Fitxer de Prevenció de Blanqueig de Capitals o La darrera versió de tots els DS és de maig de 2018.
Comentaris: • Veure punt 5.7 del present informe.

- En l'Annex 14 s'incorpora l'inventari de màquines actualitzat a abril de 2018.

- Pel que fa a l'estructura dels fitxers, en el punt 4.2 de tots els DS, excepte en el DS de Pacients, que és des del punt 4.1 al punt 4.5, es descriu l'estructura dels diferents tractaments i se n'exposa la finalitat i descripció dels sistemes d'informació que els tracten.

C. Si s'escau, mesures alternatives quan no sigui possible establir sistemes d'obertura mitjançant clau o dispositiu equivalent a les portes dels armaris, arxivadors o altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal.

Si s'escau, mesures alternatives quan els armaris, arxivadors o altres elements en què s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal no es trobin amb àrees en què l'accés estigui protegit amb portes d'accés dotades de sistemes d'obertura mitjançant clau o un altre dispositiu equivalent *(nivell alt)*.

Comentaris:

- L'Annex 30 sobre *Funcionament d'arxiu en paper* ja incorpora la informació sobre les mesures de seguretat aplicades als diferents tractaments.

D. Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit en el Reglament.

Comentari:

- L'Entitat ja disposa de diferents protocols d'actuació degudament descrits als annexos, amb formularis i indicacions d'actuació, com pot ser per la declaració d'incidències o els registres d'entrades i sortides dels dispositius i suports informàtics.

E. Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal incloses en els fitxers.

Comentaris:

- A l'Annex 39, Protocol de Bones Pràctiques pels professionals, ja es troben descrites les funcions i obligacions del personal en relació al tractament de dades de caràcter personal.

- Així mateix, en tots els DS s'exposen les obligacions del personal en el punt de *Descripció de les obligacions dels usuaris de les dades.*

F. Procediment de notificació, gestió i resposta davant les incidències.

Comentaris:

- En l'Annex 4 s'hi troba el model de notificació per les incidències.
- Així mateix, en l'Annex 32 s'exposa amb detall el circuit de notificació d'incidències.

G. Procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats.

Comentaris:

- En l'Annex 17 sobre *Sistema de seguretat i pla de contingències* es descriu el procediment de realització de les còpies de seguretat.
- Pel que fa al procediment de recuperació, l'Annex 24 sobre *procediment per recuperació de dades* exposa el procediment a seguir així com el personal encarregat de realitzar aquestes recuperacions.
- Pel que fa a les còpies de seguretat de l'aplicació GNPT realitzades per l'empresa INTEROUTER, que presta servei d'allotjament de les dades, ja s'aporta un Protocol detallat de la realització de les còpies de seguretat, tal com s'havia sol·licitat en l'anterior auditoria.

H. Mesures que sigui necessari adoptar per al transport de suports i documents, així com per a la destrucció dels documents i suports o, si s'escau, la reutilització d'aquests últims.

Comentaris:

- En tots els DS s'exposen els mecanismes de seguretat a tenir en compte en la transmissió de la informació, ja sigui de manera telemàtica o físicament.
- En l'Annex 17 sobre *sistema de seguretat i pla de contingències*, es descriuen les mesures de seguretat a tenir en compte per la destrucció de suports i papers. Així mateix, es disposa de l'Annex 45 sobre *destrucció de documents amb dades de caràcter confidencial.*

I. La identificació dels fitxers o tractaments que es tractin en concepte d'encarregat de tractament amb referència expressa al contracte o document que reguli les condicions de l'encàrrec, la identificació del responsable i del període de vigència de l'encàrrec, així com també si el tractament es realitza, o no, en els locals del responsable.

Comentari:

- L'Entitat té llistats tots els tercers encarregats de tractament, en l'Annex 44 sobre *relació de contractes de confidencialitat*.

J. Quan l'entitat actuï com a encarregat de tractament en els seus propis locals, aliens als del responsable del fitxer, ha de preveure en els documents de seguretat oportuns la identificació del fitxer o tractament i el seu responsable i les mesures de seguretat a implementar en relació amb el tractament.

Comentari:

- L'Entitat consta que actua com a encarregat de tractament de, segons s'estableix a l'Annex 46. El lloc del tractament són els mateixos locals de l'Entitat, per la qual cosa cal implementar les mesures de seguretat corresponents al nivell de seguretat corresponent. Tot i que no consta específicament el nivell de seguretat, en tractar-se de dades de pacients, s'entén que és alt.

Autoritzacions

K. Autorització per a l'emmagatzematge de dades de caràcter personal en dispositius portàtils (usuaris/ perfils d'usuaris i període de validesa).

Tractament de dades de caràcter personal en dispositius portàtils que no permetin el xifratge.

Comentaris:

- Durant els treballs de camp es s'ha detectat que s'utilitzen USB corporatius, els quals es troben custodiats per Sistemes d'Informació, de manera que cal de sol·licitar una autorització per poder-los fer servir.

- En l'Annex 47 sobre *tractament de dades de caràcter personal en dispositius portàtils*, es descriu el procediment per obtenir l'autorització per tractar dades en dispositius informàtics portàtils, com ara suports USB.

L. En relació al tractament de dades de caràcter personal fora dels locals del responsable, cal que hi hagi l'autorització, com també els usuaris/ perfils d'usuaris i el període de validesa per a aquest tractament.
Comentari: • En tots els DS, en el punt de *gestió de suports automatitzats*, s'exposa que l'execució de tractament de dades de caràcter personal fora dels locals de la ubicació del fitxer requereix una autorització expressa.
M. Personal autoritzat per concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.
Comentaris: • L'Annex 40 descriu el procediment per crear o donar de baixa una clau de pas, indicant el personal responsable o autoritzat per dur-ho a terme. • Així mateix, l'Annex 48 descriu el procediment a seguir per sol·licitar i autoritzar accessos remots. • A més, l'Annex VII del DS de GNPT descriu el procediment per donar d'alta a un usuari a dita aplicació.
N. Personal autoritzat a accedir als llocs on estiguin instal·lats els equips físics que donin suport als sistemes d'informació. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.
Comentari: • En el punt de *control i limitació d'accés físic* de tots els DS, es descriu el personal autoritzat a accedir al lloc on es troben instal·lats els equips físics que donen suport als sistemes d'informació.
O. Personal autoritzat a accedir als suports i documents que contenen dades de caràcter personal. Procediment d'accés de persones no autoritzades als espais que contenen dades de caràcter personal.
Comentaris:

• L'Annex 27 descriu el personal autoritzat a accedir a l'arxiu d'històries clíniques. • Així mateix, l'Annex 22 i 23 exposen un registre dels accessos realitzats als diferents despatxos, i de les peticions de claus per accedir-hi.
P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.
Comentaris: • En el punt de *gestió de suports automatitzats* de tots els DS es disposa que únicament quan sigui exclusivament necessari es traurà el suport automatitzat fora de l'Entitat, sempre amb les mesures de seguretat exigibles. • En el punt de *mecanismes de seguretat en la transmissió de la informació* de tots els DS, s'exposa que queda prohibit enviar dades confidencials per correu electrònic fora de la institució.
Q. Personal autoritzat per a la recepció/ enviament de dades de caràcter personal *(nivell mitjà i/ o alt).*
Comentari: • A l'Annex 13 es relaciona al personal autoritzat a enviar dades de caràcter personal.
R. Personal autoritzat per a la realització del procediment de recuperació de dades.
Comentari: • A l'Annex 24 sobre *procediment de recuperació de dades* s'exposa el personal autoritzat per a la realització del procediment de recuperació de dades.
S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.
Comentari: • Veure el punt 5.4 del present informe.

Altres mesures
T. Procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat.
Comentaris: • En l'Annex 43 sobre *Protocol d'atorgaments als professionals de claus de pas als aplicatius informàtics*, es descriu el procediment d'assignació i distribució de les contrasenyes. • D'altra banda, l'Annex 40 exposa el circuit per assignar contrasenyes, encara que res es disposa sobre l'emmagatzematge de contrasenyes.
U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.
Comentari: • L'Annex 37 exposa que la clau de pas caducarà cada 3 mesos.
V. Pel cas que es realitzin proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal amb dades reals s'ha d'anotar la seva realització al document de seguretat.
Comentari: • No consta que es realitzin proves amb dades reals.
W. Identificació del responsable de seguretat *(nivell mitjà i/ o alt)*.
Comentari: • Aquest consta en tots els DS de l'Entitat.

X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document *(nivell mitjà i/ o alt)*.
Comentaris: • En tots els DS hi ha un punt de *revisions i propostes de millora*, redirigint-se a l'Annex 6 (Excel) en què consta l'informe de revisions mensuals, i a l'Annex 17 en què consta l'informe de revisions semestrals pel que fa al procediment de còpies de seguretat. • No obstant, segons es detectà durant els treballs de camp, no es realitzen actualment revisions dels accessos de manera mensual pel que fa a l'aplicació GNPT.

Àrea de millora

▲	No detectada	*Vegeu comentaris efectuats al quadre anterior.*

5.4. Delegació d'autoritzacions.

Base legal: Article 84 RD 1720/2007.

Situació actual

Les autoritzacions que s'atribueixen al Responsable del Fitxer poden ser delegades en les persones designades en aquest efecte, algunes de les quals consten detallades en els Documents de Seguretat. A mode d'exemple comentar que:

- Autorització del responsable del fitxer a aquella persona encarregada de realitzar els procediments de recuperació de dades: en tots els DS es descriu que el responsable del fitxer delega en el responsable de seguretat la tasca de la recuperació de dades. Així mateix, es continua disposant que els responsables de seguretat deleguen la tasca de recuperació de dades a tots els treballadors del departament d'informàtica.

- Autorització per a tractar dades fora dels locals del responsable del fitxer; en tots els DS s'exposa que l'execució de tractament de dades de caràcter personal fora dels locals de la ubicació del fitxer és autoritzada expressament pel responsable del fitxer.

- En data 01/05/2018 s'ha nomenat Javier Remacha Fuentes com a Delegat de Protecció de Dades de l'Entitat, i se n'ha fet la comunicació a l'APDCat en data 11/05/2018, amb número de registre 0199/698/2018.

Àrea de millora

▲	No detectada	

5.5. Tercers.

ENCARREGATS DE TRACTAMENT

Base legal: Article 82 RD 1720/2007.

Situació actual

L'Annex 44 de *relació contractes de confidencialitat,* relaciona tots els contractes d'encarregats de tractament que té formalitzats l'Entitat.

S'ha realitzat un mostreig dels contractes facilitats per l'Entitat, passant a analitzar-ne els següents:

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
INGENIERÍA DE LA INFORMACIÓN, S.L. (IN2)	Serveis informàtics	☑	El contracte d'encarregat de tractament formalitzat amb l'Entitat compleix en gran mesura amb els requeriments de l'article 12 de la LOPD, però hi manca una definició més precisa dels serveis que presta l'encarregat i el tipus de dades a què pot accedir
GRANT THORNTON, S.L.P.	Serveis d'assessoria legal i administrativa	☑	El contracte compleix en general els requeriments previstos a l'article 12 de la LOPD. No obstant, caldria especificar les mesures de seguretat que són aplicables al tractament.
INGECAL, S.L.	Serveis d'auditoria	☑	El contracte compleix en general els requeriments previstos a l'article 12 de la LOPD. No obstant, caldria especificar les mesures de seguretat que són aplicables al tractament.
S.R.L. KINESIS	Serveis de rehabilitació mèdica i social	☑	El contracte compleix correctament els requeriments de l'article 12 de la LOPD.
INFORMÁTICA EL CORTE INGLÉS, S.A.	Serveis informàtics	☑	El contracte compleix els extrems previstos a l'article 12 de la LOPD.
ICA	Servei de software per l'aplicació Neopersonal Trainner	☑	El contracte compleix amb els extrems previstos a l'article 12 de la LOPD.

ASHO A-2, S.L.	Serveis de codificació	☑	El contracte d'encarregat de tractament formalitzat amb l'Entitat compleix en gran mesura amb els requeriments de l'article 12 de la LOPD, però hi manca una definició més precisa dels serveis que presta l'encarregat.
INSTITUT DE SERVEIS SANITARIS I SOCIALS, S.L.	Serveis d'investigació	☑	El contracte d'encarregat de tractament formalitzat amb l'Entitat compleix en gran mesura amb els requeriments de l'article 12 de la LOPD, però hi manca una definició més precisa dels serveis que presta l'encarregat.
ASOCIACIÓN FEDERAL ESPAÑOLA PARA EL FOMENTO DE LA ECONOMÍA DEL BIEN COMÚN	Serveis d'auditoria	☑	El contracte d'encarregat de tractament formalitzat amb l'Entitat compleix en gran mesura amb els requeriments de l'article 12 de la LOPD, però hi manca una definició més precisa dels serveis que presta l'encarregat.

Àrea de Millora

▲	No detectada	L'Entitat signa contractes d'encarregat de tractament i registra tots els encàrrecs i la seva vigència. En alguns casos, la informació sobre l'encàrrec no apareix completa en alguns contractes, especialment el fitxer a què s'accedirà en motiu de la prestació del servei, i les mesures de seguretat a aplicar d'acord amb el nivell de seguretat del fitxer. **Observació d'acord amb el nou RGPD**: A partir del 25 de maig de 2018 els contractes ja signats, i els darrers, amb els Encarregats dels Tractaments hauran de respectar el contingut que preveu l'article 28 del RGPD.

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

Del mostreig efectuat en destaquem els següents tercers sense accés a dades:

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPROMÍS	COMENTARIS
PREBLAU, S.R.L.	Dades control domòtic de la piscina	☑	El contracte formalitzat compleix l'article 83 del RDLOPD.
ORDENARBAL, S.L.	Servei de venta d'ordinadors i de hardware	☑	El contracte formalitzat compleix l'article 83 del RDLOPD.
ISS FACILITY SERVICES MULTISERVICIOS INTEGRALES, S.L.	Servei de neteja	☑	El contracte formalitzat compleix l'article 83 del RDLOPD.

Àrea de Millora

▲	No detectada	

5.6. Legitimació de dades.

Base legal: Articles 5 i 6 LOPD 15/1999.

Situació actual

S'analitza a continuació on s'evidencia la legitimació de les dades dels fitxers de l'entitat:

FITXER	LEGITIMACIÓ	COMENTARIS
Pacients	Als pacients que són de primera visita se'ls hi fa entrega del full d'informació i consentiment.	Aquest document compleix la normativa vigent en el moment de realitzar l'auditoria, però és millorable. En concret, no caldria demanar el consentiment per a la cessió de dades a la l'entitat pública o privada amb qui el pacient té concertada la prestació dels serveis mèdics, ja que aquesta cessió es basa en l'execució d'un contracte, si bé és correcte que se n'informi (com passa amb la cessió a la Història Clínica Compartida, la qual està habilitada per la Llei 21/2000). És correcte que es demani autorització expressa per a l'enviament d'informació sobre novetats i la revista "Sobre Ruedas". En tot cas, amb el nou RGPD, els checkboxs haurien d'incloure tant l'opció de marcar "sí" com l'opció de marcar "no", per tal que quedi clar que marcar "no" no implica cap afectació a la prestació del servei. Tot i que encara no és aplicable en el moment de realització de l'auditoria, és recomanable tenir en compte la informació exigida per l'art. 13 RGPD, que en bona part ja està proporcionant el document. Hi falta la informació sobre el dret que té l'interessat a acudir a una autoritat de control. També segons el RGPD caldria incloure-hi la base legal del tractament, que seria la pròpia prestació del servei sòcio-sanitari, i els períodes de

		conservació de les dades, que es podria fer amb una referència als períodes previstos per la legislació sanitària. En aquest document s'incorpora una autorització general per a l'ús de les dades amb finalitats de recerca i investigació. També hi ha tres autoritzacions específiques per a tractaments que excedeixen la prestació assistencial amb un checkbox que el pacient ha de marcar: per a l'enviament d'informació sobre novetats, per a l'ús de SMS per a les comunicacions i per a la recepció de la revista "Sobre Ruedas". D'altra banda, s'autoritza a que es pugui accedir a les dades de salut amb finalitats de recerca i investigació per part del propi personal de la Fundació.
Personal	L'Entitat pot rebre currículums per tres mitjans diferents: - Per email - En paper, personalment - Per correu ordinari Quan es reben per email o per correu, s'envia una resposta amb la clàusula informativa de la LOPD, que és correcte.	La resposta atorgada als currículums rebuts per correu electrònic i ordinari, pel que fa a la clàusula informativa, és correcte d'acord amb l'article 5 de la LOPD. Pel que fa a l'aplicatiu "Borsa de Treball", en registrar-se, l'usuari ha de marca un checkbox d'acceptació d'una política de privacitat, però no hi ha cap link a l'esmentada política de privacitat. Per tant, no consta que s'hagi d'acceptar una clàusula amb el contingut informatiu de l'article 5 de la LOPD. Caldria, en tot cas, que s'hagués d'acceptar una clàusula web amb aquest contingut informatiu.
	En l'Annex 25 del DS s'exposa la clàusula informativa que s'annexa en el contracte de treball que se li fa signar al treballador quan s'incorpora a l'Entitat.	Aquests documents són correctes d'acord amb la normativa en matèria de protecció de dades.
	Des de Prevenció de Riscos Laborals es lliura als treballadors un model de consentiment per a la realització de revisions mèdiques.	Aquest document és correcte.

Externs	Pel que fa els estudiants en pràctiques, s'indica que se'ls hi fa entrega del mateix full d'informació i compromís dels treballadors, així com del full de confidencialitat per a treballs d'investigació.	El document que s'entrega als estudiants és el compromís de confidencialitat, encara que aquest document hauria d'incorporar clàusula informativa d'acord amb l'article 5 de la LOPD, amb l'objectiu de legitimar les dades dels estudiants.
	En referència als estudiants de Màster, s'indica que un cop acceptada la seva preinscripció a la Universitat Autònoma de Barcelona, se'ls hi fa emplenar un imprès de matrícula. En aquest mateix formulari es preveu l'autorització de cessió de les dades a certes entitats, així com l'autorització de rebre informació promocional de l'Entitat. Un cop inscrits, se'ls hi fa entrega del mateix full d'informació i compromís de confidencialitat dels treballadors, com també del full de confidencialitat per a treballs d'investigació.	La clàusula informativa incorporada a aquest document és correcte Atès que mitjançant el document d'inscripció ja s'està legitimant el tractament de les dades dels estudiants, no caldria lliurar full d'informació. En tot cas, el procediment és correcte.
	Pel que fa als estudiants de pràctiques de la Universitat, primerament omplen el formulari d'inscripció al curs on-line anterior a la realització de les pràctiques. Un cop finalitzat el curs indicat, se'ls hi fa entrega del mateix full d'informació i compromís de confidencialitat també es lliura als treballadors.	La clàusula informativa incorporada a aquest document és correcte. Per tal com en el formulari d'inscripció ja s'estan legitimant les dades dels estudiants, no caldria lliurar un full d'informació. El procediment és correcte.
	D'altra banda, pel que fa els estudiants de programa de postgrau de Títol expert, s'entrega als estudiants el mateix full d'inscripció utilitzat pel curs on-line, així com full d'informació i compromís de confidencialitat.	La clàusula informativa incorporada a aquest~~s~~ document és correcte. Per tal com en el formulari d'inscripció ja s'està legitimant el tractament de les dades dels estudiants, no caldria lliurar un full d'informació. El procediment és correcte.

	Pel que fa als voluntaris, de Treball Social es formalitza contracte de compromís de voluntariat.	El document és correcte.
	A la pàgina web de l'Entitat es troba penjat el formulari "*Fes-te Amic de l'Institut Guttmann",* que ja inclou una clàusula d'acceptació obligada mitjançant un checkbox.	La clàusula és conforme a l'art. 5 de la LOPD. En tot cas, recomanem tenir en compte els nous requeriments informatius de l'art. 13 RGPD. D'altra banda, recomanem revisar el tractament de dades dels Aa~~a~~mics de l'~~i~~Institut Guttmann.
	Als usuaris que prestin serveis a l'Entitat en benefici de la comunitat, se'ls hi fa signar el full d'informació i compromís de confidencialitat, i el compromís de prestació de treballs.	El document és correcte, ja que compleix els requeriments de l'article 5 de la LOPD.
	Segons s'informa des del Departament de Comunicació, se li lliura al pacient autorització d'imatge de manera casuística, segons la necessitat. D'altra banda, es disposa d'autorització d'imatge pel cas de que el pacient sigui menor d'edat o incapacitat legalment, i es requereixi el consentiment dels seus representants legals.	Aquests documents són correctes d'acord amb la normativa de protecció de dades.
	Segons informen, remeten la revista "*Sobre ruedas"* als pacients que expressament ho autoritzen al full d'informació que es proporciona als pacients. També hi ha l'opció de donar-se de baixa d'aquest servei d'enviament.	Aquest procediment és correcte.
	L'Entitat fa servir diferents models d'autoritzacions d'imatge: - Autorització per la gravació de sessions formatives, per poder divulgar les imatges	Aquests models són correctes d'acord amb la normativa en matèria de protecció de dades.

	tant al canal youtube de l'Entitat, com a la intranet corporativa. - Autorització d'imatges per als treballadors i estudiants, lliurada de manera casuística.	
Reclamacions	L'Entitat disposa de formularis de reclamacions interns i exercici de drets ja adaptats al nou RGPD, perquè els pacients puguin formular queixes i/o reclamacions.	Els models utilitzats per a les reclamacions i exercici de drets són correctes.
Videovigilància	L'Entitat té càmeres de videovigilància a les entrades del centre, al hall i als diferents passadissos de la planta -2, -1 i 0. Disposen de cartells informatius indicant l'existència del tractament. Les imatges són guardades en un termini de temps no inferior a 15 dies.	Els cartells informatius, de conformitat amb la Instrucció 1/2006 de l'Agència Espanyola de Protecció de Dades, ja estan correctament disposats.
Investigació Clínica	L'Entitat fa entrega del Consentiment Informat, acompanyat d'un full informatiu, a més del qüestionari del full informatiu.	El full informatiu ja inclou una clàusula informativa que compleix els requeriments de l'article 5 de la LOPD.
GNPT	Perquè un centre sanitari o social pugui adquirir l'aplicació GNPT, haurà d'omplir un formulari d'inscripció en què caldrà indicar un professional del centre de contacte com a supervisor.	Aquest formulari ja conté una clàusula informativa que compleix els requeriments de l'article 5 de la LOPD.
	Els professionals terapeutes són els encarregats de donar d'alta als pacients a l'aplicació, havent	En el document de política de privacitat hi consta una clàusula informativa, que és conforme a l'article 5 de la LOPD.

	d'acceptar la política de privacitat un cop ja se li ha assignat un usuari.	
Administració	No ha quedat acreditat que es proporcioni la informació sobre el tractament de dades de clients o proveïdors.	Cal que l'Entitat incorpori avisos legals també relatius al tractament de dades personals de clients i/o proveïdors, a efectes de prestació de serveis i gestió administrativa. Es recomana incloure un avís legal per capes en el model de factura, per exemple, per complir amb el deure d'informació respecte a clients.

Àrea de Millora

●	Àrea de Millora	**Observació d'acord amb el nou RGPD:** Segons els criteris manifestos per les diferents Agències, les institucions que hagin legitimat correctament les dades a partir de l'article 5 de la LOPD, amb l'entrada en vigor de la normativa europea, hauran de legitimar igualment totes les dades que tracten a partir dels articles 13 i 14 del RGPD. S'aconsella a l'Entitat la revisió de les clàusules d'acord amb la normativa europea.

5.7. Drets ARCO.

Base legal: Articles 15-17 LOPD 15/1999.

Situació actual

En el punt 4.9 de tots els DS, excepte els DS d'Investigació i de GNPT, en què es troba en el punt 4.11, es descriu el procediment d'exercici dels drets d'accés, rectificació, cancel·lació i oposició de dades. Així mateix, l'Annex 7 inclou tots els formularis d'exercici dels drets esmentats, ja adaptats al nou RGPD.

Des de la Unitat d'Atenció al Client, s'informa que, per a sol·licitar documentació mèdica, el circuit a seguir és el següent:

- El pacient realitza la sol·licitud mitjançant el formulari de "*sol·licitud de documentació mèdica"*, el qual es troba a la zona d'admissions de l'Entitat.
- Aquesta sol·licitud és gestionada des d'admissions, recopilant-se la documentació mèdica requerida, entregant-se aquesta al pacient des de la mateixa zona d'admissions.
- Segons s'indica, el termini màxim de resposta d'aquestes peticions és de 30 dies, fent signar un document conforme s'ha lliurat aquesta documentació al pacient.

Respecte a la resta de drets ARCO, no consta que se n'hagi rebut cap sol·licitud d'exercici, encara que el circuit seria el mateix, i es tramitaria remetent el formulari de sol·licitud al Delegat de Protecció de Dades.

Àrea de millora

▲	No detectada	Els models de què disposa l'Entitat per a l'exercici dels drets, ja adaptats al nou RGPD, són correctes. El procediment també és correcte. **Observació d'acord amb el nou RGPD:** A més de considerar la modificació de les clàusules de legitimació de dades d'acord l'article 13 del RGPD, l'Entitat ha de tenir en compte les modificacions entorn dels terminis de resposta (art. 12.3 RGPD) i la regulació dels nous drets (art. 15 al 22 del RGPD)

II - BLOC DE MESURES INFORMÀTIQUES

5.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'Entitat disposa del servidor local a les seves instal·lacions en què s'allotgen les dades del gestor assistencial, de les carpetes en xarxa i del correu electrònic. Pel que fa a les dades de RRHH, la part de nòmines es troba allotjada als servidors de l'empresa INTEGRO, i la part de gestió horària es troba allotjada als servidors de l'empresa SOFTMACHINE. En referència a l'aplicació GNPT (exercicis de rehabilitació), l'allotjament de les dades és en els servidors de l'empresa INTEROUTER.

Respecte a la seguretat dels equips, aquests tenen instal·lat l'antivirus McAfee. Així mateix, es disposa de dos Firewalls.

L'Entitat presenta un total de 254 SAI (sistema d'alimentació ininterromput), o grups electrògens, per tal de donar resposta en cas de fallida d'electricitat.

Les aplicacions detectades durant el treball de camp utilitzades per l'Entitat, a través de les quals es tracten dades de caràcter personal són:

APLICACIÓ	UTILITAT
CURS CLÍNIC	Gestió assistencial
ADMISSIONS	Gestió de les primeres visites i agenda dels pacients
AGENDA PACIENTS	Gestió i organització de les activitats terapèutiques ocupacionals i fisioterapeutes dels pacients
INTEGRO	Gestió de les nòmines de RRHH
MOODLE	Gestió de formació
SAP	Comptabilitat
GNPT	NeuroPersonalTrainer (exercicis de rehabilitació)
CAU	Centre d'atenció a l'usuari i gestió de peticions

Pel que fa al sistema de carpetes, l'Entitat presenta un sistema de carpetes en xarxa Departamentals, així com un sistema de carpetes individuals segons el professional.

Pel que fa el correu electrònic, tots els treballadors tenen compte de correu electrònic individual, encara que a més es disposa d'una relació de comptes de correus genèrics per Departaments.

Àrea de millora

▲	No detectada	

5.9. Connexions remotes.

Base legal: Article 86 RD 1720/2007.

Situació actual

L'Annex 38 conté una relació d'usuaris amb accés remot a les diferents bases de dades o a l'equip, que ja indica el motiu pel qual es té accés remot, com també les mesures de seguretat aplicades.

Segons s'informa durant els treballs de camp, tots els treballadors tenen accés via web tant al correu electrònic, com a la intranet i al gestor horari de treballadors. Per poder tenir accés remot al curs clínic o a l'equip, cal ser autoritzat per Gerència i habilitat expressament pels Sistemes d'Informació.

D'altra banda, els diferents proveïdors que tenen accés remot a les bases de dades concretes, es troben relacionats a l'Annex 38 esmentat. Aquest accés és sempre amb la prèvia autorització de l'Entitat, atorgant accés mitjançant VPN només al programa o base de dades concreta que correspongui.

Àrea de millora

▲	No detectada	

5.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

Durant els treballs de camp es comenta que sempre que es remeten documents amb dades de caràcter personal de nivell alt, es fa a través d'un procés d'encriptació o dissociació. Segons el punt 4.8.6 del DS de Pacients, l'enviament de dades de pacients és mitjançant PDF xifrats amb l'algoritme AES 128 o AES 256, i amb el Winzip, amb algoritme AES 256.

Segons mostreig aportat per l'Entitat, la versió de l'Adobe Acrobat i del Winzip xifra els PDF mitjançant l'algoritme AES 256 bits.

Des de Treball Social s'indicà que, per raó de les derivacions de pacients a centres sociosanitaris, residències o centres de dia, es remeten els informes socials als diferents centres via correu electrònic, mitjançant PDF amb contrasenya.

Així mateix, des d'Admissions, es comentà que en el cas de que el pacient sol·liciti còpia d'un informe, aquest se li remet via correu electrònic, mitjançant PDF amb contrasenya.

D'altra banda, des del Departament de facturació es remeten els informes mèdics addicionals sol·licitats per les Mútues de trànsit, mitjançant correu electrònic, en un PDF amb contrasenya.

Àrea de Millora

▲	No detectada	

5.11. Control d'accés.

Base legal: Articles 89.1, 91 i RD 1720/2007.

Situació actual

De conformitat amb el punt 4.8.3.1 del DS de Pacients, es dóna accés a les persones autoritzades amb un sistema de perfils d'usuaris, amb drets d'accés, de grup i per especialitat, el qual permet acotar i limitar l'accés a les dades.

El gestor assistencial Curs Clínic, presenta un accés limitat per permisos atorgats segons els perfils per grups i especialitats, com ara, per exemple:

- Auxiliar de Farmàcia
- Auxiliar d'infermeria
- Professionals assistencials
- Administrador

Per mitjà de l'Annex 18 es disposa d'un Directori d'usuaris actius, tan pel que fa al curs clínic com al sistema de carpetes i a la resta de bases de dades, en què es detallen els diferents permisos assignats.

Pel que fa a la base de dades d'Admissions, només el personal d'admissions pot gestionar les agendes i primeres visites, mentre que la resta de professionals només poden consultar. Segons es va informar, a tall d'exemple, les infermeres només poden visualitzar els pacients una setmana abans de la seva visita programada, i una setmana després d'aquesta, bloquejant-se l'accés al pacient un cop passat aquest termini. Els diferents perfils i permisos atorgats són:

- Infermeria
- Metges
- Fisioterapeutes
- Treball Social
- Psicòlegs
- Logopedes

Pel que a la base de dades d'Agenda de pacients, el seu accés és també limitat per permisos atorgats segons els perfils professionals.

En referència a l' aplicació GNPT (aplicació d'exercicis de rehabilitació), el circuit per donar-se d'alta és el següent:

- Respecte als diferents centres que volen incorporar l'aplicació GNPT a la seva Entitat, l'empresa ICA és l'encarregada de donar d'alta al professional supervisor designat per cada centre, el qual haurà d'omplir el formulari d'inscripció, generant-se un nou usuari i remetent l'aplicació automàticament una contrasenya a aquest supervisor, la qual haurà de modificar.

- L'usuari supervisor serà l'encarregat de donar d'alta al professional terapeuta a l'aplicació, generant-se un nou usuari i remetent-se automàticament una contrasenya que s'haurà de canviar.

- El mateix procediment es segueix per donar d'alta a l'aplicació a un pacient: el professional terapeuta és l'encarregat de donar d'alta el pacient com a usuari, moment en què se li envia automàticament una contrasenya que haurà de ser modificada.

Per donar d'alta a un nou usuari que s'incorpora a l'Entitat, des del Departament de RRHH, mitjançant l'aplicació "*Clau de pas",* li atorguen un perfil genèric al Curs Clínic. És des de RRHH que es defineix el perfil de cada usuari, i se li assignen els accessos corresponents. En aquest sentit, remeten correu electrònic a Sistemes d'Informació amb el perfil del treballador, per tal de que li donin d'alta al correu electrònic, i a la xarxa. En cas de que l'usuari requereixi un accés o permís concret o més específic, el Director d'Àrea ho haurà de comunicar a Sistemes d'Informació perquè ho gestioni. En l'Annex 11 es descriu el procediment per donar d'alta a un nou usuari i per l' atorgament de claus de pas. La primera contrasenya s'ha d'anar a buscar personalment i es lliura dins un sobre.

Pel que fa al sistema de baixa, el circuit és el mateix que s'acaba d'exposar.

Àrees de millora

▲	No detectada	**Recomanació:** A partir del dia 25 de maig de 2018 serà aplicable el Reglament General de Protecció de Dades. Aquest Reglament incorpora els principis de protecció de dades des del disseny i per defecte. En base a aquest principi, és necessari que, a l'hora de donar d'alta els usuaris, la opció predefinida sigui aquella que faciliti un accés més restringit a les dades, podent habilitar un perfil d'usuaris amb més permisos d'accés, i no al contrari com es realitza en l'actualitat.

5.12. Identificació i autenticació d'usuaris.

Base legal: Articles 93 i 98 RD 1720/2007.

Situació actual

A l'Annex 40 i 43 es descriu el procediment d'assignació d'usuaris i claus de pas als professionals de l'Entitat.

Pel que fa al Curs Clínic, cada professional disposa d'un sistema de credencials individual, de manera que coincideix la complexitat de la contrasenya amb la base de dades d'Admissions, i amb l'aplicació de l'Agenda de pacients. La contrasenya és d'un mínim de 8 dígits, amb combinació de majúscules i minúscules, alfanumèrica, i presentant una periodicitat de caducitat de 90 dies. Així mateix, presenta un sistema de bloqueig per intents d'accés erroni, al tercer intent, es bloqueja l'equip durant 30 minuts, i a partir del sisè intent, la contrasenya ha de ser restablerta per l'administrador del sistema. D'altra banda, presenten un sistema de bloqueig de pantalla, que s'activa als 2 minuts d'inactivitat. .

Pel que fa a l'INTEGRO, també es requereix un usuari i contrasenya per accedir-hi, de manera que la contrasenya ha de ser d'un mínim de 8 dígits, amb combinació de majúscules i minúscules, i caduca un cop l'any. D'altra banda, s'informa que el sistema de bloqueig per inactivitat és configurable i que, per tant, no tots els equips el tenen activat.

Pel que fa a GNPT, el seu accés és també mitjançant un sistema de credencials individual per pacients i per professionals. La complexitat de la contrasenya requereix d'un mínim de 8 dígits, amb combinació de majúscules i minúscules, alfanumèrica i caduca un cop l'any. Així mateix, presenta un sistema de bloqueig per intents d'accés erroni, al tercer intent, així com un sistema de bloqueig per inactivat als 5 minuts.

Es comentà que les primeres contrasenyes adjudicades als usuaris de la GNPT s'obliguen a modificar, encara que no succeeix el mateix amb la resta d'aplicacions, en la que simplement es recomana la seva modificació.

Pel que fa els comptes de correu electrònics genèrics, s'indicà que s'hi accedeix mitjançant el sistema de credencials individual adjudicat a cada usuari. Per tant, s'identifica degudament al treballador quan envia un correu electrònic des del compte de correu genèric, constant la signatura de cada professional.

Àrea de Millora

▲	No detectada	*Es recomana seguir aquestes directrius, per definir les contrasenyes com a segures:* • *No repetir contrasenya anterior.* • *Periodicitat de canvi, mínim cada 6 mesos.* • *Bloqueig al tercer intent erroni de validar-se al sistema.* • *Bloqueig en cas de desús per part de l'usuari (5-10 minuts), per tal de que es requereixi la introducció de nou dels noms d'usuari i claus de pas per a reiniciar l'activitat en aquells equips que tinguin accés a dades personals.*

		D'altra banda, és recomanable que s'obligui als usuaris a modificar la primera contrasenya adjudicada, per tal de garantir la deguda confidencialitat de la contrasenya i la identificació inequívoca i personalitzada dels usuaris.

5.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

Segons el punt 4.8.7.2 del DS de Pacients, el punt 4.10.3 del DS d'Investigació i el punt 4.10.3 del DS de GNPT, els programes disposen del corresponent registre dels accessos.

El gestor assistencial Curs Clínic, base de dades gestora també del fitxer d'investigació, presenta un registre d'accessos, mitjançant la pestanya *"Seguiment Accessos",* en què es permeten conèixer tots els requeriments de l'article 103 del RDLOPD.

Es realitzen revisions dels registres d'accessos de manera mensual pel cap de Sistemes d'Informació, que es remeten al Delegat de Protecció de Dades.

D'altra banda, l'aplicació GNPT du a terme un registre d'accessos, en què es permet conèixer la data i hora de l'accés, com el professional que ha accedit, però no es pot conèixer el fitxer a què s'ha accedit ni el tipus d'accés.

S'informa d'una nova aplicació, anomenada CAU, de què disposen tots els usuaris de l'Entitat dins el directori actiu. A través d'aquesta aplicació, és possible gestionar les entrades i sortides de dispositius, les peticions, la programació de tasques, etc.

	No detectada	Cal que el Delegat de Protecció de Dades continuï revisant almenys una vegada al mes la informació de control registrada mitjançant el registre d'accessos i elabori un informe de les revisions realitzades i els problemes detectats.

5.14. Còpies de seguretat.

Base legal: Articles 94, 102 i 112 RD 1720/2007

Situació actual

En l'Annex 17 *"Sistema de seguretat i pla de contingències"* es descriu el procediment de realització de les còpies de seguretat. Pel que fa a la descripció del procediment de recuperació de dades i comprovacions de les còpies, l'Annex 24 descriu de manera detallada aquest procediment de recuperació de dades.

Les còpies de seguretat es realitzen de manera diària, mitjançant granges de disc i DVD, els quals s'allotgen a la sala on es troba el servidor. De manera paral·lela, es realitzen còpies de seguretat diàries remotes, mitjançant l'empresa EID o Valora Data, externalitzant-se les còpies mitjançant un sistema de *cloud,* de forma que resten allotjades físicament en servidors de l'empresa.

Pel que fa al procediment de recuperacions de dades, s'indica que es realitzen a petició de l'usuari i cada 15 dies, documentant-se com a una incidència i aportant-se mostreig per l'Entitat.

Pel que fa a les dades de l'aplicació GNPT, aquestes estan allotjades en els servidors de l'entitat INTEROUTER, i es realitzen còpies de seguretat de manera diària, mitjançant una cabina externa de discs. Els procediments de còpia i recuperació estan descrits en un protocol elaborat per l'Entitat pel març de 2017 i proporcionat a efectes d'auditoria. Aquests procediments també es descriuen al punt 4.5.4 del DS de GNPT, encara que durant els treballs de camp s'indica que les recuperacions de dades només es realitzen a petició de l'usuari i no de manera periòdica.

Àrea de millora

▲	No detectada	De conformitat amb l'article 94.3 del RDLOPD, el responsable del fitxer de verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de seguretat i de recuperació de les dades.

5.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

És inherent al funcionament de qualsevol entitat la generació de fitxers ofimàtics paral·lels, i més si es té en compte que es disposa de Microsoft Office en els equips de l'entitat.

En tot cas, no consten fitxers o tractaments temporals.

Àrees de millora

▲	No detectada	

5.16. Registre d'entrades i sortides de suports automatitzats.

Base legal: Article 97 RD 1720/ 2007.

Situació actual

En tots els DS es disposa que en els casos en que l'Entitat utilitzi suports informàtics es complimentarà un registre d'entrades i sortides per garantir el control i la seguretat de les dades del fitxer. Així mateix, l'Entitat presenta l'Annex 47 sobre "*Tractament de dades de caràcter personal en dispositius portàtils",* en el que es descriu el procediment per obtenir l'autorització per tractar dades fora dels locals de l'Entitat.

Segons es c

omenta des de Sistemes d'Informació, es disposa de dispositius USB corporatius, els quals es presten a sol·licitud de l'usuari, registrant-se la seva entrega en el programa de CAU.

Així mateix, existeix la possibilitat de que els equips siguin extrets dels locals de l'Entitat per qüestions de manteniment i reparacions. Des de Sistemes d'Informació, es guarda una traçabilitat d'aquestes sortides mitjançant el seu registre al programa CAU de gestió de peticions.

Durant els treballs de camp es detectà que certs equips portàtils han sigut adjudicats a cers professionals per tasques o feines puntuals. Aquests equips poden sortir dels locals de l'Entitat, no obstant, no es preveu en el DS cap punt de sortides periòdiques autoritzades.

Àrees de millora

▲	No detectada	

III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS

5.17. Dispositius portàtils, inventari, etiquetatge, xifrat i destrucció de suports i documents.

Base legal: Articles 86, 92, 101 i 112 RD 1720/ 2007.

Situació actual

L'Entitat disposa d'ordinadors portàtils assignats a certs professionals per tasques puntuals o temporals, els quals poden sortir fora dels locals de l'Entitat.

Així mateix, es constata l'existència de dispositius USB corporatius, que es troben a Sistemes d'Informació amb un mecanisme de xifrat i poden ser sol·licitats pels usuaris que els vulguin utilitzar. D'altra banda, es detecten dispositius tablets assignats a determinats professionals.

Tots els equips, suports i dispositius amb dades de caràcter personal es troben inventariats, i la seva assignació es troba registrada al programa CAU. Tots els equips, suports i dispositius estan etiquetats amb números correlatius.

Pel que fa a la destrucció documental, a la zona d'admissions i als controls d'infermeria es disposa d'una caixa tancada amb clau en la què es llencen els documents destinats a ser destruïts mitjançant les destructores que es troben a la zona d'admissions, gerència i alguns dels despatxos

Pel que fa a la reparació dels equips, aquesta és duta a terme per Sistemes d'Informació a les mateixes instal·lacions de l'Entitat. No obstant, hi ha casos en què es preveu la sortida dels equips per ser reparats fora de les instal·lacions de l'Entitat, per una empresa externa, encara que s'indicà que aquesta situació és puntual.

En referència a la destrucció d'aquests, es comenta que es procedeix a formatar el disc dur a les mateixes instal·lacions.

Àrees de millora

▲	No detectada	

5.18. Control d'accés.

Base legal: Articles 99, 107, 108 i 111 RD 1720/ 2007.

Situació actual

Pel que fa l'accés al servidor de l'Entitat, aquest es troba en una sala destinada exclusivament a la seva custòdia, degudament condicionada i tanca amb clau. S'indica que només hi té accés autoritzat el personal de Sistemes d'Informació, acompanyant al personal de manteniment i de neteja en cas de que hi hagin d'accedir. Segons s'informa, en cas que sigui necessari accedir a la sala del servidor i no hi hagi personal de Sistemes d'Informació, a la zona de porteria del centre es registrarà aquest accés, ja que caldrà sol·licitar-ne la clau.

Des del Departament d'Arxiu, es comenta que tenen implementat un circuit o procediment de sol·licitud d'HC, el qual es basa en les següents directrius:

- El professional mèdic de l'Entitat sol·licita l'HC que necessita al Departament d'Admissions, ja sigui per finalitats assistencials o per a recerca.
- Des d'aquest Departament, es registra la petició al programa de gestió d'HC, fent constar-hi el professional sol·licitant, la data en que s'ha proporcionat l'HC i de quina HC es tracta.
- Es du un control de les HC que es troben fora de l'arxiu, mitjançant el mateix programa indicat, realitzant-se de manera periòdica un control de les HC que no han sigut retornades.

L'arxiu d'HC i de documentació mèdica es troba a la planta -2, en una sala destinada només a la seva custòdia, formant aquesta documentació el full d'informació i consentiment del pacient i el seu consentiment informat, ja que la resta de documentació és informatitzada. Aquesta sala es troba tancada amb clau, sent custodiada a la zona d'admissions, sent el personal autoritzat a accedir-hi el d'admissions, els metges de guàrdia i el personal d'infermeria. Així mateix, la sala disposa d'un sistema de doble porta i reixa d'accés.

Pel que fa a la documentació mèdica dels pacients que es troben hospitalitzats, aquesta és custodiada en el control d'infermeria de la planta on es trobi. Un cop és donat d'alta, la documentació es trasllada al Departament d'admissions, en què digitalitzaran tota la documentació que consti i guardaran en paper només el full d'informació i consentiment de pacient i el consentiment informat, a banda de les proves que només puguin conservar-se en suport documental. Aquesta documentació serà trasllada a la sala d'arxiu de la planta -2.

Pel que fa a les reclamacions i sol·licituds de proves dels pacients, aquestes són emmagatzemades al mateix Departament d'admissions, en un armari dotat de mecanismes que impedeixen la seva obertura mitjançant clau.

Des del Departament d'Investigació i Recerca es comenta que la documentació dels assaigs i estudis es troba adjuntada a l'HC assistencial del pacient, la qual es troba emmagatzemada a la sala d'arxiu comentada de la planta -2. Pel que fa a la documentació dels estudis actius, indicaren que és custodiada als despatxos dels diferents Investigadors Principals, en armaris tancats amb clau, encara que no es va poder comprovar.

Pel que fa a la documentació de Treball Social, formada pels informes socials dels pacients, la documentació dels voluntaris i dels usuaris que ofereixen serveis en benefici de la comunitat,

tant l'actiu com el passiu es troba emmagatzemada al despatx del Departament de Treball Social, en armaris tancats amb clau, trobant-se així mateix la porta d'accés al despatx tancada amb clau.

Pel que fa els expedients dels treballadors, aquests es troben al despatx del Departament de RRHH, en un armari tancat amb clau així com la porta d'accés al despatx. Respecte al passiu, aquest és traslladat a una sala d'arxiu de la planta -2 destinada només a la custòdia de documentació de RRHH, en arxivadors tancats amb clau, així com la porta d'accés a la sala d'arxiu.

Des del Departament de Formació, s'indicà que la documentació i expedients dels diferents estudiants, tant de Màster com de MIR, pràctiques i de postgrau, es troba emmagatzemada al Departament de Docència, en uns arxivadors tancats amb clau, com també és tancada la porta d'accés al Departament.

Pel que fa a la documentació de facturació, aquesta es troba tota informatitzada, i no es conserva en paper.,

D'altra banda, segons s'indica des del Departament d'Admissions, en cas que acudeixi al centre qualsevol persona preguntant per si un pacient es troba ingressat o no, sense comprovar la seva identitat, se li informa de l'habitació en que es troba el pacient, en cas de que efectivament es trobi ingressat a l'Entitat.

Àrea de millora

▲	No detectada	*Pel que fa a la informació atorgada a les persones que acudeixen al centre preguntant per si un pacient es troba ingressat, abans de donar-li dita informació i de indicar-li quina habitació ocupa, se li hauria de preguntar al pacient si és del seu interès que es comuniqui el seu ingrés a qualsevol persona que acudeixi a preguntar, d'acord amb els criteris de l'Agencia Española de Protección de Datos.*

5.19. Registre d'accessos.

Base legal: Article 113 RD 1720/2007.

Situació actual

Segons el punt 4.8.4 del DS de Pacients, i el punt 4.5.2 del DS d'Investigació, el Departament de Serveis Generals, a través dels guàrdies de seguretat, porta un registre de tots els accessos físics que es realitzen als despatxos que normalment es troben tancats amb clau. A l'Annex 23 hi ha un control dels diferents accessos realitzats als diferents despatxos, i en l'Annex 22 hi ha una taula de control de claus, en què es pren nota de la persona o servei que sol·licita la clau d'accés a qualsevol despatx o sala d'arxiu.

D'altra banda, en el cas de que qualsevol professional vulgui accedir a una HC, ho haurà de sol·licitar prèviament al Departament d'Admissions, guardant-se registre de les adjudicacions.

Àrees de millora

▲	No detectada	

5.20. Criteris d'arxiu.

Base legal: Articles 106 RD 1720/2007.

Situació actual

Els criteris d'arxiu garanteixen la correcta conservació de la documentació, la localització i consulta de la informació i possibiliten l'exercici dels drets d'oposició al tractament, accés, rectificació i cancel·lació.

Fitxer de Pacients: Pel que fa a la documentació mèdica, s'informa que l'única documentació que es custodia en paper és el full d'informació i consentiment del pacient, el seu consentiment informat i les proves que només puguin conservar-se en suport documental. Així doncs, la documentació mèdica custodiada en paper es troba emmagatzemada a la sala d'arxiu de la planta -2, seguint un criteri d'arxiu per número d'història clínica, sense diferenciar-se entre actiu i passiu. El criteri per ser considerada la documentació com a passiva és que el pacient sigui èxitus, sent custodiada aquesta de manera indefinida. El responsable de l'arxiu és la cap del Departament d'admissions.

Pel que fa a la documentació mèdica dels pacients que es troben hospitalitzats, aquesta es troba emmagatzemada en els controls d'infermeria de les diferents plantes, sent el criteri d'arxiu per número d'habitació.

En referència a la documentació de Treball Social, es troba emmagatzemada en el despatx del Departament de Treball Social, sent el seu criteri d'arxiu per Departaments, el servei i per data, sense diferenciar-se entre actiu i passiu. Pel que fa al passiu, aquest és custodiat al mateix despatx, de manera indefinida. El responsable d'aquest arxiu és la cap de Treball Social.

Fitxer d'Investigació i Recerca: Pel que fa a la documentació d'investigació i recerca, aquesta es troba custodiada juntament amb la HC dels pacients, la qual es troba emmagatzemada a la sala d'arxiu esmentada de la planta -2. El criteri d'arxiu d'aquesta coincideix amb l'exposat del fitxer de pacients, és a dir, per número d'història clínica, custodiant-se la documentació de manera indefinida. En referència a la documentació de recerca, pel que fa a les HC dels estudis que es troben actius, aquestes es custodien als despatxos dels Investigadors Principals, encara que no es va poder constatà el seu criteri d'arxiu.

Fitxer Externs: La documentació i expedients dels estudiants, es troba custodiada al Departament de Docència, seguint un criteri d'arxiu diferenciat segons l'especialitat de l'estudiant, això és: el criteri d'arxiu de la documentació dels estudiants MIR, és per any i data, i el de la resta d'estudiants, és per número de matrícula. Així mateix, s'organitzen en diferents carpetes segons sigui MIR, pràctiques, postgrau o Màster. El passiu és custodiat en el mateix Departament, amb el mateix criteri d'arxiu indicat, de manera indefinida. La responsable de l'arxiu és la cap del Departament de Docència.

En quan a la documentació dels usuaris que presten serveis a l'Entitat en benefici de la comunitat i dels voluntaris, es troba custodiada en el despatx del Departament de Treball Social, seguint el mateix criteri d'arxiu indicat en el fitxer de pacients. Això és, per Departaments, per servei i per data, sense diferenciar-se entre actiu i passiu. En quan al passiu, aquest és custodiat al mateix despatx, de manera indefinida. El responsable d'aquest arxiu és la cap de Treball Social.

Fitxer de Personal: Pel que fa als expedients dels treballadors, aquests es troben al despatx del Departament de RRHH, seguint un criteri d'arxiu per ordre alfabètic, i diferenciant-se segons

sigui contractació temporal o indefinida. En quan al passiu, és custodiat en una sala d'arxiu de la planta -2, seguint el mateix criteri d'arxiu, custodiant-se de manera indefinida. El responsable de l'arxiu és la cap de RRHH.

Fitxer de Reclamacions: En referència a les reclamacions dels pacients, aquestes són custodiades al Departament d'Admissions. El criteri d'arxiu és per anys. La responsable de l'arxiu és la cap de Departament d'Admissions.

Fitxer d' Administració: Pel que fa a la facturació, tota la documentació es troba informatitzada. No es disposa de documents en format paper.

Àrees de millora

▲	No detectada	

5.21. Entrades i sortides de documents.

Base legal: Articles 97 i 114 RD 1720/2007.

Situació actual

A l'Annex 3 consta una taula en format Excel per al registre de sortides de documents de l'Entitat, segons requeriments de l'article 97 del RDLOPD.

Des del Departament d'Arxiu i Admissions comenten que, en cas de que un pacient sol·liciti còpia de qualsevol informe mèdic, se li fa signar en el moment de la recollida document conforme s'ha entregat aquest informe. D'aquesta manera, s'anota la seva recollida en el mòdul de gestió de sol·licituds d'informes del programa d'admissions. L'Entitat aporta mostres d'aquesta traçabilitat.

Des d'aquest mateix Departament, s'informa que poden rebre derivacions des de diferents centres sanitaris, enviant-se a l'Entitat els informes mèdics i volants dels pacients. En el programa d'admissions es guarda traçabilitat d'aquestes recepcions, i queda constància de tots els extrems que preveu la normativa.

Pel que fa a la facturació, s'indica que els informes mèdics addicionals que sol·liciten les Mútues de Trànsit, són enviats mitjançant correu ordinari. Segons comentaren, es guarda traçabilitat mitjançant l'anotació de la sortida en el mòdul comentat de gestió de sol·licituds d'informes del programa d'admissions.

Àrea de millora

▲	No detectada	

5.22. Fitxers temporals.

Base legal: Articles 87 i 112 RD 1720/2007.

Situació actual

Es detecta durant els treballs de camp que és possible la generació de fitxers temporals, en el context de l'activitat mèdica diària de l'Entitat, encara que és té plena consciència de que, un cop finalitzada la tasca per la qual s'ha generat el document, aquest ha de ser destruït mitjançant les eines de què disposen, d'acord amb que s'ha detallat en el punt 5.17 d'aquest Informe.

Des de RRHH es comenta que els currículums en paper es guarden durant 6 mesos.

Àrees de millora

▲	No detectada	

IV- BLOC DE MESURES ORGANITZATIVES

5.23. Registre d'incidències.

Base legal: Articles 90 i 100 RD 1720/2007.

Situació actual

En tots els DS es preveu el procediment de notificació i gestió de les incidències, indicant-se que en l'Annex 4 es troba el model de formulari de notificació d'incidències. A l'Annex 32 es descriu amb més detall el procediment de notificació d'incidències.

Segons indicaren durant els treballs de camp, el circuit de notificació d'incidències és el següent:

- El treballador remet un correu electrònic a Sistemes d'Informació, informant de la incidència, o directament la registra mitjançant el programa CAU.

- La incidència queda registrada al programa, de forma que se'n pot saber la data de notificació, la naturalesa de la incidència, la categoria, la persona que l'ha notificat, la data de resolució i el tècnic que l'ha resolt. Segons s'indica, cada 6 mesos es remet una relació de les incidències al Delegat de Protecció de Dades.

Àrees de millora

▲	No detectada	**Observació d'acord amb el nou RGPD**: Amb l'entrada en aplicació del RGPD a partir del 25 de maig de 2018, si es produeix una violació de la seguretat, el responsable l'ha de notificar a l'autoritat de control en un termini màxim de 72 hores, tret que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones. A més, quan sigui probable que la violació comporti un alt risc per als drets de les persones interessades, el responsable l'ha de comunicar a les persones afectades sense dilacions indegudes i en un llenguatge clar i senzill, tret que: • El responsable hagi adoptat mesures de protecció adequades, com ara que les dades no siguin intel·ligibles per a persones no autoritzades. • El responsable hagi aplicat mesures posteriors que garanteixen que ja no hi ha la probabilitat que es concreti l'alt risc. • Suposi un esforç desproporcionat

5.24. Difusió de funcions i obligacions.

Base legal: Article 89.2 RD 1720/2007.

Situació actual

L'Entitat posa en coneixement tant de professionals com dels col·laboradors un *"Protocol de Bones Pràctiques Dades Caràcter Personal 2016-2019",* que es troba a l'Annex 39, en què es descriuen les funcions i obligacions de tot el personal respecte a la seguretat i el tractament de dades de caràcter personal, amb incidència també en les conseqüències d'un incompliment.

Pel que fa a la formació, s'informa des de RRHH que, quan un treballador s'incorpora a l'Entitat, ha de cursar diferents cursos a través de la plataforma Moodle i examinar-se'n dels continguts. Aquests continguts corresponen a: responsabilitat corporativa i compliance, actuació en cas d'emergència, medi ambient, prevenció de riscos laborals, plànols, bones pràctiques, seguretat i protecció de dades. Al cap de 3 setmanes, se'ls passa una enquesta per comprovar la seva comprensió dels cursos.

Àrea de Millora

▲	No detectada	

6. CONCLUSIONS

Avaluats tots els punts determinats pel Reglament de desenvolupament de la Llei orgànica 15/1999, de protecció de dades de caràcter personal, després de realitzar les actuacions corresponents a les diferents dependències de l'entitat i participar en les entrevistes amb els corresponents responsables d'àrea, i havent-se valorat també la documentació aportada i els sistemes de tractament de la informació, l'equip auditor detecta que les àrees de millora i salvetats, de conformitat amb l'establert al RDLOPD, són:

ÀREES DE MILLORA
I- BLOC GENERAL
5.2. Aspectes generals.
5.6. Legitimació de dades.
III- BLOC DE MESURES FÍSIQUES O DOCUMENTALS
No es detecten.

SALVETATS
I- BLOC GENERAL
No es detecten.
II- BLOC DE MESURES INFORMÀTIQUES
No es detecten.

Barcelona, 19 de juny de 2018.

Pere Ruiz Espinós

- Soci -