

ÍNDEX

ÍNDEX	1
1. OBJECTIUS I CONTINGUT	2
2. METODOLOGIA	3
3. DADES DE L'ENTITAT I TREBALLS EFECTUATS	4
3.1. Dades identificatives.....	4
3.2. Treballs efectuats.....	4
4. SIMBOLOGIA	6
5. ANÀLISI DE LES DIFERENTS ÀREES DE L'AUDITORIA	8
I - BLOC GENERAL	8
5.1. Auditoria.....	8
5.2. Aspectes generals.....	9
5.3. Document de seguretat.....	10
5.4. Delegació d'autoritacions.....	18
5.5. Tercers.....	19
5.6. Legitimació de dades.....	22
5.7. Drets ARCO.....	24
II - BLOC DE MESURES INFORMÀTIQUES	25
5.8. Accés a xarxes.....	25
5.9. Connexions remotes.....	26
5.10. Transmissions per xarxes de telecomunicacions.....	27
5.11. Control d'accés.....	28
5.12. Identificació i autenticació d'usuaris.....	29
5.13. Registre d'accessos.....	30
5.14. Còpies de seguretat.....	31
5.15. Fitxers temporals suport automatitzat.....	32
5.16. Registre d'entrades i sortides de suports automatitzats.....	33
III- BLOC DE MESURES FÍSQUES O DOCUMENTALS	34
5.17. Dispositius portàtils, inventari, etiquetatge, xifrat i destrucció de suports i documents.....	34
5.18. Control d'accés.....	35
5.19. Registre d'accessos.....	36
5.20. Criteris d'arxiu.....	36
5.21. Entrades i sortides de documents.....	37
5.22. Fitxers temporals.....	38
IV- BLOC DE MESURES ORGANITZATIVES	39
5.23. Registre d'incidències.....	39
5.24. Difusió de funcions i obligacions.....	40
6. CONCLUSIONS	41

I. Objectius i contingut

De conformitat amb el que estableix la normativa vigent sobre protecció de dades¹, 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 SL* 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	Coordinació Logística Sanitària, AIE
NIF	V64118276
Domicili	C/ Catalunya, s/n. 08130- Santa Perpètua de Mogoda (Barcelona)

3.1.2. Descripció de l'activitat

Coordinació Logística Sanitària, A.I.E., es va constituir l'any 2006. Actualment està integrada per Corporació Sanitària Parc Taulí, Consorci Mar Parc de Salut de Barcelona, Institut de Prestacions d'Assistència Mèdica al Personal Municipal i Prestacions d'Assistència Mèdica S.L

CLS, A.I.E, és una plataforma logística que presta als seus socis serveis logístics integrals en material fungible sanitari i no sanitari.

L'objecte social es limita exclusivament a desenvolupar activitats econòmiques auxiliars a les desenvolupades pels seus membres relacionades amb l'emmagatzematge i logística dels materials, béns i documentació, i en especial:

- Activitats de planificació, coordinació i execució conjunta de tasques de recepció, comprovació, classificació, emmagatzematge, packaging, organització, distribució i lliurament a punt de destí de les mercaderies de tot tipus que precisi la prestació de les activitats dels socis.
- Activitats d'arxiu, emmagatzematge, custòdia, organització i lliurament al centre d'origen, quan sigui necessari, de les històries clíniques en format físic i que tinguin la consideració de passiu i/ o semipassiu en funció de la data de la darrera consulta efectuada sobre la mateixa o de la seva casuística en funció d'altres factors objectius.
- Qualsevol altra d'anàloga naturala.

3.2. Treballs efectuats.

S'han realitzat els treballs de camp de l'auditoria en els diversos serveis i àrees de Coordinació Logística Sanitària:

- Àrea de Sistemes d'Informació
- Àrea de Recursos Humans
- Àrea de Recepcions i Coordinador d'Històries Clíniques
- Àrea d'Expedicions
- Àrea de Logística Interna

- Àrea de Facturació

Pel que fa a espais físics, a més de les àrees indicades, s'han revisat els següents: sala CPD, despatx de Recursos Humans, despatx de Facturació i instal·lacions on es troben emmagatzemades les històries clíniques.

3.2.1. Data de realització de l'auditoria

Dia	23 de febrer de 2017
------------	----------------------

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. Jordi Herrera	Responsable de Sistemes d'Informació
2	Sra. Montse López	Responsable de Recursos Humans
3	Sra. Maribel Gonzalez	Responsable de Recepcions i Coordinadora d'Històries Clíniques
4	Sra. Adela Alonso	Responsable d'Expedicions
5	Sr. Julio Oya	Responsable de Logística Interna
6	Sr. Jaime Aracil	Responsable de Finances

Relació de la documentació lliurada a l'auditor:

Document
Organigrama
Estatuts
Cartes de l'Agència Espanyola de Protecció de Dades amb els codis d'inscripció dels fitxers
Documents de seguretat i annexos
Esquema xarxa informàtica




Inventari d'equips
Usuaris aplicacions
Esquemes de xarxa
Manual de Bones Pràctiques
Circuit i formularis d'exercici drets ARCO
Registre d'incidències
Registre d'entrada i sortida de suports
Contractes

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
	<i>No detectada</i> , és a dir, la situació actual de l'Entitat compleix la normativa.
	<i>Àrea de millora</i> , és a dir, l'estat de la situació actual requereix ésser completat perquè no s'ajustaria íntegrament a l'establert a la normativa.
	<i>Salvetat</i> , 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

Coordinació Logística Sanitària, AIE, en endavant l'Entitat, va realitzar la darrera auditoria en matèria de protecció de dades el març de 2015, complint amb les previsions legalment establertes en l'article 96 del RDLOPD, segons el que es preveu el criteri de biennialitat en la realització d'auditories.

L'Entitat ha aportat un informe on es detallen les àrees de millora i salvetats, estant signat pel Responsable de Seguretat i la Responsable del Fitxer. En conclusió, podem afirmar que queda constància que es van elevar les conclusions a la responsable del fitxer perquè adoptés les mesures correctores adequades.

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	TRACTAM ENT
Recursos Humans	2112791764	Realització dels processos habituals de gestió de Recursos Humans i pagament de nòmines, així com de la prevenció de riscos laborals.	Alt	Mixt
Administració	2112791765	Gestió habitual dels processos d'administració, facturació i comptabilitat.	Bàsic	Mixt
Videovigilància	2112800127	Videovigilància de les instal·lacions	Bàsic	Automatitzat

Àrees de millora

	No detectada	<i>No es detecten tractaments diferents dels esmentats que comportin la modificació dels fitxers preexistents, tampoc la creació de nous fitxers.</i>
---	--------------	---

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.
<u>Comentaris:</u> <ul style="list-style-type: none">• L'Entitat ha elaborat un DS per tots els fitxer que té inscrits: fitxer de Recursos Humans, Fitxer d'Administració i Fitxer de Videovigilància.• L'última versió dels DS és de febrer de 2017.
B. Àmbit d'aplicació del document amb especificació detallada dels recursos protegits: <ul style="list-style-type: none">○ Inventari de suports.○ Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten.
<u>Comentaris:</u> <ul style="list-style-type: none">• L'Entitat disposa d'inventari de suports però no es troba annexat als DS.• En el punt 2 del DS es descriu l'estructura dels fitxers.

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*).

Comentari:

- Manca establir les mesures de seguretat en relació a l'arxiu d'històries clíniques, atès que no disposen de mecanismes de tancament suficients.

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

Comentari:

- En el DS s'hi troben diferents procediments d'actuació. Manca regular el procediment a seguir pel cas que s'hagin d'enviar documentació amb dades de caràcter personal de nivell alt per correu electrònic.

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

Comentaris:

- Es regula en el punt 4 "*Organització de la seguretat*" del DS, diferenciant entre responsable del fitxer, usuaris, encarregats de tractament i tercers sense accés a dades.
- Així mateix l'Entitat disposa del Manual de Bones Pràctiques pels empleats.

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

Comentaris:

- Consta en el punt 5.7.1 *Registre d'incidències* del DS.
- L'explicació de la notificació, gestió, resposta i registre d'incidències s'amplia en l'annex 12 "*Procediment de notificació, gestió i resposta davant les incidències*".

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

Comentari:

- Es troba regulat en el punt 5.3 anomenat "*Procediment, periodicitat i custòdia per a la realització de còpies de seguretat*" del DS. Així mateix l'Entitat disposa d'un document on es detalla els horaris de les còpies de seguretat, tot i que no es troba annexat al Document de Seguretat.

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:

- Els mecanismes de seguretat i la transmissió d' informació es troben definits en el punts 5.5 “*Mecanismes de seguretat en la transmissió de la informació del DS*”, tot i que caldria especificar quin mecanisme de seguretat és utilitzat pel que fa als enviaments de documentació amb dades de caràcter personal a través de correu electrònic.
- En el punt 5.9.1 del DS es regula el procediment de destrucció o la reutilització dels suports electrònics.
- Pel que fa al suport paper, en el punt 5.9.2 del DS s'estableix que es disposa d'una destructora per eliminar la documentació amb dades de caràcter personal que ja no és necessària.

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.

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:

- En el punt I del DS es fa constar que l'Entitat és encarregada de tractament de Corporació Sanitària Parc Taulí i Consorci Mar Parc Salut de Barcelona, en relació al fitxer de pacients d'ambdues entitats.

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.

Comentari:

- L'Entitat ho regula en el punt 5.2 del DS, en concret en l'apartat 9, indicant que els usuaris tenen prohibida l'exportació d'arxius de l'Entitat a dispositius portàtils. En el cas que fos necessari cal que es sol·liciti al responsable de Sistemes d'Informació o Responsable de Seguretat.

L. En relació al tractament de dades de caràcter personal fora dels locals del responsable, cal que hi hagi l'autorització així com també els usuaris/ perfils d'usuaris i el període de validesa per a aquest tractament.

Comentari:

- Es detalla en el punt 5.8 "*Règim de treball fora dels locals de la ubicació dels Fitxers*".

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.

Comentari:

- Es preveu en el punt 5.1 del DS, indicant que el responsable de Sistemes d'Informació assigna permisos i perfils d'accés, prèvia comunicació de la responsable de l'Àrea de Recursos Humans.

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:

<ul style="list-style-type: none"> • Consta en el punt 5.1 "Definició de les normes i procediments de seguretat" del DS
<p>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.</p>
<p><u>Comentari:</u></p> <ul style="list-style-type: none"> • En el punt 2.5 del DS es regula l'accés i manteniment de les dades en el fitxer, fent una remissió al punt 5.1 del mateix DS i indicant les persones autoritzades per cadascun dels fitxers.
<p>P. Autorització per a les sortides de suports i documents, inclosos els compresos i/ o annexos a un correu electrònic.</p>
<p><u>Comentari:</u></p> <ul style="list-style-type: none"> • En el punt 9 del DS la Responsable del Fitxer autoritza les sortides de suports i documents, inclosos els compresos en correus electrònics, amb l'única finalitat de desenvolupar l'activitat de l'Entitat.
<p>Q. Personal autoritzat per a la recepció/ enviament de dades de caràcter personal (nivell mitjà i/ o alt).</p>
<p><u>Comentari:</u></p> <ul style="list-style-type: none"> • En el punt 9 del DS consta que s'autoritza al responsable de Recursos Humans per tal que s'encarregui de la recepció i del lliurament de documents i suports que continguin dades de caràcter personal.
<p>R. Personal autoritzat per a la realització del procediment de recuperació de dades.</p>
<p><u>Comentari:</u></p> <ul style="list-style-type: none"> • En el punt 9 s'autoritza al responsable de sistemes per tal que verifiqui cada 6 mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de seguretat i recuperació de dades.

S. Persones en qui el responsable del fitxer ha delegat les autoritzacions que a ell li corresponen.
<u>Comentari:</u>
<ul style="list-style-type: none"> • Veure 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.
<u>Comentaris:</u>
<ul style="list-style-type: none"> • Es troba regulat en el punt tercer del punt 5.2 del DS.
U. Periodicitat de canvi de les contrasenyes d'accés al sistema i a les aplicacions.
<u>Comentari:</u>
<ul style="list-style-type: none"> • La caducitat de la contrasenya es regula en el punt 5.2 apartat 5 del DS, indicant que la contrasenya caduca cada 365 dies, tot i que aquest criteri no s'adapta a la realitat. En conseqüència cal modificar aquest punt.
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.
<u>Comentari:</u>
<ul style="list-style-type: none"> • Consta en el punt 5.6 "<i>Proves amb dades reals</i>" del DS.
W. Identificació del responsable de seguretat (<i>nivell mitjà i/ o alt</i>).

Comentari:

- No consta en cap punt.

X. Els controls periòdics que s'han realitzat per verificar el compliment del que disposa el document (*nivell mitjà i/ o alt*).

Comentari:

- Es regula en el punt 8 del “*Revisió mensual del sistema de protecció de dades*” del DS. En l'annex 14 s'hi troba el model d'informe de revisió mensual del sistema

Àrea de millora

●	Àrea de millora	Respecte els DS existents, cal que s'acabin de detallar els punts comentats en el quadre anterior. Cal annexar el model per l'exercici del dret d'oposició.
---	-----------------	--


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 el Document de Seguretat. Per exemple en el punt 9 hi consten diferents autoritzacions. En primer lloc s'autoritza al responsable de sistemes a verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de seguretat i recuperació de dades. En segon lloc s'autoritza a la responsable de Recursos Humans perquè s'encarregui de la recepció i del lliurament de documents i suports que continguin dades de caràcter personal.

Àrees de millora

	No detectada	
---	--------------	--

5.5. Tercers.

ENCARREGATS DE TRACTAMENT




Base legal: Article 82 RD 1720/2007.

Situació actual


L'Entitat disposa d'un llistat on consten identificats els tercers encarregats de tractament.

En el punt I del Document de Seguretat s'indica que l'Entitat és encarregada de tractament de Corporació Sanitària Parc Taulí i Consorci Mar Parc Salut de Barcelona, al custodiar l'arxiu d'històries clíniques passives i semi passives dels seus pacients.

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

ET's DETECTATS	SERVEI PRESTAT	CONTRACTE	COMENTARIS
SERVIGEST EMPRESARIAL, SL.	Assessorament empresarial, S.L.		No disposen de contracte d'encarregat de tractament d'acord amb les previsions de l'article 12 de la LOPD, atès que manca indicar les mesures de seguretat que l'encarregat de tractament està obligat a aplicar. Així mateix en el punt K del contracte s'indica el termini de 30 dies perquè l'encarregat de tractament comuniqui l'exercici dels drets ARCO a l'Entitat.
HOSTALIA	Hosting del correu electrònic. Subcontrata a ACENS		No disposen de contracte d'encarregat de tractament d'acord amb les previsions de l'article 12 de la LOPD. El document aportat no està firmat per cap de les dues parts.
MDL, DISTRIBUCIÓN LOGÍSTICA, S.A.	Transport d'històries clíniques		No disposen de contracte d'encarregat de tractament d'acord amb les previsions de l'article 12 de la LOPD atès que manca indicar les mesures de seguretat que l'encarregat de tractament està obligat a aplicar.

Salvetat

	Salvetat	<p>Cal que en el llistat on es relacionen els tercers encarregats de tractament, es faci constar fitxer al que s'accedeix, data de signatura del contracte i subcontractació, si s'escau.</p> <p>Cal que en els contractes d'encarregat de tractament s'estableixin les mesures de seguretat que l'encarregat de tractament està obligat a implementar d'acord amb el fitxer al que s'accedeix. Amb posterioritat als camps de treball, es treballa el model de contracte d'encarregat de tractament, introduint les mesures de seguretat.</p> <p>Així mateix cal un termini menor per comunicar els exercicis de drets ARCO, atès que si es determina un termini de 30 dies serà complicat que l'Entitat compleixi amb la obligació de contestar a l'interessat les sol·licituds d'exercici del dret d'accés. Pel que fa al dret de rectificació, cancel·lació i oposició resultarà impossible complir amb l'obligació legal atès que la normativa indica un termini de resposta de 10 dies.</p>
---	----------	---

PRESTACIONS SENSE ACCÉS A DADES

Base legal: Article 83 RD 1720/2007.

Situació actual

L'Entitat informa que des de l'última auditoria disposen de dos nous proveïdors que per prestar el servei pactat no hagin d'accedir a les dades de caràcter personal però sí a les dependències de l'entitat.

TERCERS SENSE ACCÉS	SERVEI PRESTAT	COMPR OMÍS	COMENTARIS
BARNARACK	Manteniment de alarma	<input checked="" type="checkbox"/>	Disposen de compromís de confidencialitat d'acord amb l'article 83 del RLOPD.
CIRERA	Gestió de residus	<input checked="" type="checkbox"/>	Disposen de compromís de confidencialitat d'acord amb l'article 83 del RLOPD.

Àrees 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
Recursos Humans	L'Entitat entrega el document “ <i>Full d'Informació de l'Empleat</i> ” en el primer contacte amb el pacient.	Aquest document és correcte per complir amb el deure d'informació regulat en l'article 5 de la LOPD.
	L'Entitat rep CV presencialment, entregant a la persona un document de resposta. Així mateix l'Entitat disposa d'un document de resposta per processos de selecció.	Aquest document és correcte per complir amb el deure d'informació regulat en l'article 5 de la LOPD.
	Pel que fa a salut laboral, l'Entitat entrega al treballador un document en el que pot acceptar la realització de la revisió mèdica.	Aquest document incorpora una clàusula que és correcte per complir amb el deure d'informació regulat a l'article 5 de la LOPD.
	Es disposa de formularis per exercir el dret d'accés, rectificació i cancel·lació.	En tots els formularis manca la clàusula que estableixi els paràmetres establerts en l'article 5 de la LOPD, per complir amb el deure d'informació regulat en el mateix.
Videovigilància	L'Entitat disposa de càmeres que enfoquen l'entrada de l'edifici, però no es visualitza la via pública.	Els cartells informatius són correctes per complir amb l'article 12.6 de la Instrucció 1/2009.

Àrea de Millora

	Àrea de Millora	Veure comentaris del quadre anterior.
---	-----------------	---------------------------------------

5.7. Drets ARCO.

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

Situació actual

El procediment d'exercici dels drets ARCO es troba esmentat en el punt 6.1 "Dret d'accés, rectificació, cancel·lació i oposició". Així mateix l'Entitat disposa dels models per l'exercici del dret d'accés, rectificació i cancel·lació, no trobant-se el d'oposició.

Durant els treballs de camp s'informà que no s'ha rebut cap sol·licitud d'exercici de dret ARCO.

Àrea de millora

●	Àrea de millora	Tot i que amb posterioritat als treballs de camp l'Entitat aportà el model de sol·licitud d'exercici de dret d'oposició, fent-lo constar també en la pàgina web, durant els treballs de camp es detectà la necessitat de disposar d'aquest model.
---	-----------------	---

II - BLOC DE MESURES INFORMÀTIQUES

5.8. Accés a xarxes.

Base legal: Article 85 RD 1720/2007.

Situació actual

L'Entitat disposa de quatre servidors ubicats en les mateixes instal·lacions de l'Entitat.

Pel que fa al tipus de xarxa disposen de tres *routers*. Hi ha línia de fibra òptica així com línia ADSL a les oficines. Pel que fa als dispositius situats al magatzem, disposen de xarxa sense fils.

En quant a la seguretat dels equips aquests tenen instal·lat l'antivirus McAfee, Windows Defender i Avast, respectivament. No hi ha cap criteri per establir quin antivirus s'instal·la a cadascun dels equips. Pel que fa a Firewall, l'Entitat disposa el propi de Windows.

L'Entitat disposa de dos SAIS (sistema d'alimentació ininterromput), per tal de donar resposta en cas de fallida d'electricitat.

Pel que fa al sistema de carpetes, l'Entitat presenta un sistema de carpetes en xarxa departamentals. L'accés a les carpetes és limitat segons la categoria professional. També hi trobem carpetes en xarxa personals dels professionals.

Pel que fa al correu electrònic és extern, considerant que el servei de *hosting* el presta l'empresa Hostalia. Cal apuntar que no tots els treballadors disposen de compte de correu electrònic. Únicament en disposen els professionals de serveis generals i quatre persones de magatzem.

Les aplicacions detectades durant el treball de camp utilitzades per l'Entitat i en les quals es tracten dades de caràcter personal es detallen a continuació:

APLICACIÓ	UTILITAT
INFORMIX	Aplicació de gestió d'històries clíniques
BODEC	Gestió de Recursos Humans
CONTAPLUS	Gestió comptable
TICKETING	Comunicació i gestió d'incidències

Àrees de millora

	No detectada	
---	--------------	--

5.9. Connexions remotes.

Base legal: Article 86 RD 1720/2007.

Situació actual

L'Entitat informà de que els treballadors no poden accedir des de fora dels locals de l'Entitat a les diferents aplicacions.

Únicament accedeix de manera remota el Responsable de Sistemes d'Informació per realitzar tasques de manteniment i solucionar possibles incidències. L'accés remot és a través de Team Viewer o bé, a través de l'eina Guacamole en que l'accés és a través de la pàgina web sent la connexió xifrada, sent necessari usuari i contrasenya per accedir-hi.

D'altra banda, es comentà que l'empresa informàtica externa SEIDOR accedeix al servidor on s'emmagatzemen les dades del *Carrusel*, no trobant-se dades de caràcter personal en aquest.

Àrea de millora

	No detectada	
---	--------------	--

5.10. Transmissions per xarxes de telecomunicacions.

Base legal: Article 104 RD 1720/2007.

Situació actual

En el punt 5.5 “*Mecanismes de seguretat en la transmissió de la informació*” s’indica que l’enviament de documents amb dades de caràcter personal de nivell alt cal garantir la seva confidencialitat.

S’indicà que actualment l’Entitat no realitza enviament amb dades de caràcter personal de nivell alt ni per correu electrònic ni per fax.

Àrees de millora

	No detectada	
---	--------------	--

5.11. Control d'accés.

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

Situació actual

En el punt 5.1 del DS es pot trobar una relació dels usuaris autoritzats a l'accés a les dades per cadascun dels fitxers.

Així mateix en l'annex 19 s'indiquen els diferents perfils existents en l'Informix, Bodec i HCIS. Les aplicacions presenten un accés limitat per permisos atorgats segons els perfils establerts per grups i categories professionals.

Les funcions i obligacions dels perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació es troben definides segons el perfil professional i el rol que desenvolupa dins de l'entitat.

Per donar d'alta un nou treballador, la responsable de Recursos Humans ho comunica al responsable de Sistemes d'Informació on s'indica nom, cognom i el lloc de treball que ocuparà, del perquè aquest li doni d'alta a les corresponents aplicacions, al sistema Windows, a les carpetes compartides necessàries i al correu electrònic.

Pel que fa al sistema de baixa i modificació es segueix el mateix circuit. El termini per donar de baixa a l'usuari és immediat.

Àrees de millora

	No detectada	
---	--------------	--

5.12. Identificació i autenticació d'usuaris.

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

Situació actual

Tot el personal amb accés al sistema i als programes disposa d'usuari i contrasenya, de manera que es garanteix la correcta identificació i autenticació dels usuaris. La identificació de qualsevol usuari per accedir al sistema i als programes és inequívoca i personalitzada.

La contrasenya per accedir a l'entorn Windows té set dígitos com a mínim, no havent obligacions de que sigui alfanumèrica. Aquesta caduca cada any. L'Entitat disposa d'un sistema de bloqueig per inactivitat als quinze minuts així com un sistema de bloqueig per intent d'accés erroni al cinquè intent. Amb posterioritat als treballs de camp l'Entitat ha establert que les contrasenyes tinguin com a mínim vuit dígitos.

Pel que fa a l'Informix, el professional disposa d'usuari i contrasenya individual per accedir-hi. Pel que fa la complexitat de la contrasenya aquesta es crea per defecte. Aquesta caduca cada any, no podent-se repetir les tres últimes contrasenyes. Indicaren que hi ha instaurat un sistema de bloqueig per inactivitat que s'activa als quinze minuts. L'Entitat disposa d'un sistema de bloqueig per intent d'accés erroni al cinquè intent.

En relació a la contrasenya de Bodec aquesta és creada per defecte, no podent-se establir criteris. Aquesta caduca cada any. Indicaren que tenen instaurat un sistema de bloqueig per inactivitat que s'activa als quinze minuts. L'Entitat disposa d'un sistema de bloqueig per intent d'accés erroni al cinquè intent.


S'indicà que es disposa d'un doble sistema de validació, és a dir, es requereix un usuari i contrasenya per accedir a l'entorn Windows, i un altra contrasenya per accedir a les aplicacions.

Pel que fa a l'HCIS s'indica que el Parc Sanitari Taulí proporciona una contrasenya però que aquesta és modificada pels usuaris.

Pel que fa als comptes de correus electrònics, existeix un compte de correu electrònic genèric però que està redireccionat a un de personal, així que únicament es pot donar resposta des d'aquest compte personal.

L'Entitat informà que no és guarda un llistat de les contrasenyes de forma intel·ligible.

Àrees de millora

	Àrea de millora	<p>Es recomana que les contrasenyes compleixin els següents requisits:</p> <ul style="list-style-type: none">• Tenir una longitud mínima de vuit caràcters, tot i que amb posterioritat als treballs de camp s'ha modificat la política de seguretat de les contrasenyes per accedir al sistema, havent l'obligació de que tinguin com a mínim vuit dígitos.• Incloure caràcter de tres de les següents categories:<ul style="list-style-type: none">○ Majúscules (de la A a la Z)○ Minúscules (de la A a la Z)○ Dígitos de base 10 (del 0 al 9)
---	-----------------	---

		<ul style="list-style-type: none"> ○ Caràcters no alfanumèrics (per exemple: !, &, #, +...) • Periodicitat de canvi, mínim cada 12 mesos. • Bloqueig al tercer intent erroni de validar-se al sistema. <p>Cal que les contrasenyes, mentre estan vigent, s'emmagatzemin de forma intel·ligible.</p> <p>Amb posterioritat als treballs de camp s'ha treballat en aquest àmbit.</p>
--	--	--

5.13. Registre d'accessos.

Base legal: Article 103 RD 1720/2007.

Situació actual

Cal indicar que no es disposen de bases de dades automatitzades de nivell alt, en conseqüència no és d'aplicació aquest punt de l'informe.

Àrees de millora

	No detectada	
---	--------------	--

5.14. Còpies de seguretat.

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

Situació actual

En l'annex 5.3 del Document de Seguretat es descriu en detall el procediment de realització de les còpies de seguretat.

En aquest s'indica que es realitza una còpia completa, cada setmana, del disc dur del servidor. Així mateix es realitza una còpia diferencial de dilluns a dijous en un disc dur extern situat al CPD de les instal·lacions de l'Entitat, és a dir que en aquest es van replicant les còpies que es realitzen.

Durant els treballs de camp s'informà que cada dos dies es trasllada la informació a un disc dur o USB, i cada setmana s'emmagatzema a l'eina *Dropbox* com a mecanisme d'externalització de còpies de seguretat.

Pel que fa a l'aplicació Bodec, es fa una còpia cada hora al servidor, realitzant-se posteriorment una d'incremental. Així mateix l'aplicació realitza una còpia diària de la que també es fa una segona còpia en el servidor.

Segons s'indicà, de totes les còpies es realitza un procés de comprovació atès que el programa que realitza les còpies té incorporat aquest sistema de comprovació. En el cas que es produís alguna incidència el sistema envia un correu electrònic a l'empresa externa.

Així mateix, durant els treballs de camp, el responsable de Sistemes d'Informació revisa cada sis mesos les còpies de seguretat.

Àrees de millora

●	Àrea de millora	En relació a la utilització de Dropbox com a eina d'emmagatzemament cal fer referència al dictamen CNS 57/2013 de l'Autoritat Catalana de Protecció de Dades que estableix que les dades emmagatzemades als serveis "Dropbox" seran tractades amb garanties i condicions de seguretat que poden resultar insuficients. Així mateix es determina que l'ús d'aquesta eina i les diferents aplicacions i plataformes que permeten l'accés i la gestió d'arxius poden presentar certes vulnerabilitats. Cal que quedi constància de les revisions semestrals de les còpies de seguretat.
---	-----------------	---

5.15. Fitxers temporals suport automatitzat.

Base legal: Article 87 RD 1720/2007.

Situació actual

En el punt 8 de mesures informàtiques del Manual de Bones Pràctiques queda constància de que els fitxers temporals que continguin dades de caràcter personal cal que siguin destruïts.

Durant els treballs de camp no es detectà que els diferents professionals treballassin amb documents dels que no es fes còpia d'aquests a les carpetes en xarxa del servidor ni tampoc que arxius temporals quedessin guardats fora dels llocs que ofereixen seguretat.

Àrees de millora

	No detectada	
---	--------------	--

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


Base legal: Article 97 RD 1720/ 2007.

Situació actual

El punt 5.7.2 del DS regula el registre d'entrada i sortides de suports informàtica a l'exterior.

Durant els treballs de camp, no es detectaren moviments de suports amb dades de caràcter personal de nivell mitjà o alt, ja que no s'utilitzen USB corporatius amb dades de caràcter personal que puguin sortir del centre. Tot i així l'Entitat disposa d'un registre d'entrada i sortida de suports, en el que consta el tipus de suport, data i hora, emissor, número de suports, tipus d'informació que contenen, forma d'enviament i la persona responsable de la recepció.

Àrees de millora

	No detectada	
---	--------------	--

III- BLOC DE MESURES FÍSQUES 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 de tres ordinadors portàtils, però es comentà que no s'extreuen de les instal·lacions de l'Entitat.

Es comentà que no s'utilitza dispositius USB, trobant-se les obertures dels equips obertes.

Tots els equips es troben inventariats, així com etiquetats. S'aportà mostreig per l'Entitat de l'inventari dels equips informàtics, podent-se observar el següents camps: ID, element, marca, data d'alta, data de baixa i nom de l'equip.

Pel que fa a la destrucció de documentació, l'Entitat disposa d'una destructora al departament de Recursos Humans, atès que gran part de la documentació amb dades de caràcter personal es troba en aquest departament.

Pel que fa a la reparació dels equips s'encarrega el propi responsable de sistemes d'informació o bé una empresa externa, RICOH, depenent de l'aparell que s'hagi de reparar.

Durant els treballs de camp s'informà que encara no s'ha destruït cap equip.

Àrees de millora

	No detectada	
---	--------------	--

5.18. Control d'accés.

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

Situació actual

Pel que fa l'accés al servidor de l'Entitat, aquest es troba en una sala degudament tancada amb clau i condicionada. S'indicà que només hi té accés el responsable de sistemes d'informació, disposant únicament ell de clau per accedir-hi.

És important indicar que les històries clíniques que l'Entitat emmagatzema com a encarregat de tractament, es troben en un espai que es pot accedir des d'una altra nau de l'Entitat. Entre la nau adjunta i l'espai on s'arxiven les històries clíniques no hi ha cap porta amb mecanisme de tancament amb clau per evitar els accessos no autoritzats, tot i que es troben uns cartells informant que únicament pot accedir personal autoritzat. Així mateix hi ha una porta que dona a l'exterior de l'edifici.


Concretament, les històries clíniques es troben en caixes obertes en prestatgeries també obertes, així mateix les històries passives o semipassives es troben en sobres oberts i també en prestatgeries obertes.

Durant els treballs de camp es comprovà que els professionals del departament de Digitalització guarden les proves en armaris tancats en clau, indicant que el despatx queda tancat en clau. A mesura que les proves van sent digitalitzades es posen en unes gàbies obertes.

En quant a la documentació de Recursos Humans, els expedients dels treballadors es troben emmagatzemats al despatx del departament de RRHH, degudament tancat amb clau, en armaris tancats així mateix amb clau. Pel que fa a la documentació dels treballadors inactius es troba en una caixa oberta dins del mateix armari.

Pel que fa a la documentació de facturació i comptabilitat, aquesta es troba a l'àrea de facturació, en armaris degudament tancats amb clau.

Salvetat

	Salvetat	<p>Cal que els dispositius d'emmagatzemament de les històries clíniques disposin de tancament que obstaculitzi la seva obertura.</p> <p>Així mateix cal que les àrees on es troben aquests dispositius d'emmagatzemament estigui protegida amb portes d'accés amb sistema d'obertura mitjançant clau i un altre mecanisme equivalent. A més, aquestes àrees han de mantenir-se tancades sempre que no sigui necessari sempre que no es necessiti accedir a les històries clíniques.</p>
---	----------	---

5.19. Registre d'accessos.


Base legal: Article 113 RD 1720/2007.

Situació actual

Pel que fa a la sala de servidors únicament té claus per accedir-hi el responsable de sistemes d'informació, atès que és l'única persona que hi pot accedir.

Durant els treballs de camp s'indicà que únicament poden accedir a l'arxiu de les històries clíniques aquelles persones autoritzades. Tot i així, l'Entitat no disposa de cap mecanisme que permeti identificar els accessos que s'han realitzat.

Salvetat

	Salvetat	Cal que l'Entitat estableixi un mecanisme permeti identificar els accessos realitzats a documents que poden ser utilitzats per varies persones.
---	----------	---

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: L'arxiu actiu d'històries clíniques es troba emmagatzemat en un magatzem a les mateixes instal·lacions de l'Entitat. En aquest trobem les històries clíniques dels pacients de la Corporació Sanitària Parc Taulí i Consorci Mar Parc Salut de Barcelona. Són els responsables dels fitxers qui comuniquen quan destruir històries clíniques.

Les històries clíniques semipassives estan ordenades pels tres últims dígits del número d'història clínica. Les històries clíniques passives segueixen un criteri d'arxiu temporal, és a dir a mesura que arriben a l'Entitat es posen en caixes en ordre d'arribada.

Fitxer de Recursos Humans: Pel que fa els expedients dels treballadors, l'arxiu actiu es troba en un armari al despatx de la responsable de Recursos Humans. Aquest segueix un criteri d'arxiu per ordre alfabètic. En quant al passiu, aquest es troba en una caixa dins del mateix armari, seguint el mateix criteri d'arxiu. L'Entitat indicà que a data de l'auditoria encara no s'ha destruït documentació.

Fitxer d'Administració: Pel que fa a la documentació d'administració es troba en un armari al despatx del responsable de Facturació, ordenant-se per proveïdors i no havent-se eliminat encara cap documentació.

Àrees de millora

	No detectada	
---	--------------	--

5.21. Entrades i sortides de documents.

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

Situació actual

Totes les històries clíniques que l'Entitat disposa es fan constar a l'aplicació INFORMIX, podent observar la ubicació i el codi.


Quan una entitat demana alguna història clínica ho fa a través de l'aplicació SGA, on s'indica el número d'història clínica. Per les sortides d'històries clíniques també es segueix el mateix procés.

Durant els treballs de camp s'indicà que per les entrades d'històries clíniques es rep un llistat amb tots els números d'històries clíniques així com amb el nom del pacient, per poder fer una comprovació.

Pel que fa a les proves digitalitzades l'Entitat disposa d'un registre on es poden observar els següents camps: data d'entrada a CLS, data prova, número d'història clínica, data digitalització i el tipus de prova que es digitalitza.

En relació a la documentació relacionada amb recursos humans s'informà que l'Entitat disposa d'un registre on queda constància del tipus de suport, data i hora d'entrada, receptor, número de suports, contingut, entrada o sortida i responsable de recepció.

Àrees de millora

	Àrea de millora	Pel que fa a les entrades i sortides d'històries clíniques, tot i que el sistema del que disposa l'Entitat permet registrar les d'entrades i sortides cal establir un sistema de registre d'entrada i sortida de suports que permeti, directa o indirectament, conèixer el tipus de document, la data i hora, l'emissor, el número de documents inclosos en l'enviament, el tipus d'informació que conté, la forma d'enviament i la persona responsable de la recepció o entrega que haurà d'estar degudament autoritzada.
---	-----------------	--

5.22. Fitxers temporals.

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

Situació actual

En el punt 17 del Manual de Bones Pràctiques s'estableix que els fitxers temporals de caràcter personal han de ser destruïts i no ser guardats si no es que siguin totalment necessari per la seva posterior utilització.

Es detectà durant els treballs de camp que és possible la generació de fitxers temporals, en el context de l'activitat diària de l'Entitat, encara que es té plena consciència de que, un cop finalitzada la tasca per la qual s'ha generat el document, aquest ha de ser destruït mitjançant la destructora que disposen.

Des del departament de Recursos Humans s'informà que utilitzen documents on consenten els noms, les hores extres realitzades i la quantitat de diners que correspon pagar per aquestes hores extres. Quan ja no és d'utilitat aquest document s'informà que s'estripa, sense utilitzar-se la destructora.

Àrees de millora

●	Àrea de millora	Tot i que sigui de manera puntual el fet d'estripar documents amb dades de caràcter personal, és necessari indicar que cal procedir a la destrucció per evitar l'accés a la informació continguda en aquests o per la seva posterior recuperació.
---	-----------------	---

IV- BLOC DE MESURES ORGANITZATIVES

5.23. Registre d'incidències.

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


Situació actual

En el punt 5.7.1 del DS regula el registre d'incidències. Així mateix l'Entitat disposa de l'annex 12 on es descriu la notificació, gestió, resposta i registre de les incidències.

Segons s'indicà, l'Entitat disposa de l'eina Ticketing en la que queda constància de totes les incidències produïdes.

Durant els treballs de camp s'indica que si no es localitza una història clínica es posen en contacte mitjançant correu electrònic amb el responsable d'històries clíniques de l'entitat corresponent, no quedant traçabilitat.

Salvetat

	Salvetat	Cal que es disposi d'un registre d'incidències en el que consti el tipus d'incidència, el moment en que s'ha produït o detectat, la persona que realitza la notificació, a qui es comunica la incidència, els efectes que s'han derivat de la mateixa i les mesures correctores aplicades.
---	----------	--

5.24. Difusió de funcions i obligacions.


Base legal: Article 89.2 RD 1720/2007.

Situació actual

L'Entitat entrega als treballadors el “Manual de Bones Pràctiques de l'Empleat”, en el que consten les funcions i les obligacions del personal. Així mateix s'indiquen les conseqüències en cas d'incompliment. Durant els treballs de camp s'informà que una còpia signada és pels treballadors i un altre és per l'Entitat.

Pel que fa a la formació, es comentà que no s'ha rebut formació relativa a Protecció de Dades de Caràcter Personal.

Àrea de Millora

	No detectada	<i>Es recomana a l'Entitat que organitzi anualment una jornada o sessió en matèria de protecció de dades per als seus professionals.</i>
---	--------------	--

6. CONCLUSIONS

Inspeccionats tots els punts determinats pel Reglament de desenvolupament de la Llei orgànica 15/1999, de protecció de dades de caràcter personal, havent-se dut a terme les actuacions a les diferents dependències de l'entitat, realitzades les entrevistes amb els corresponents responsables d'àrea, havent-se valorat la documentació aportada, avaluats 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
5.3 Document de seguretat
5.6. Legitimació de dades
5.7. Drets ARCO
II- BLOC DE MESURES INFORMÀTIQUES
5.12 Identificació i autenticació d'usuaris
5.14 Còpies de seguretat
III- BLOC DE MESURES FÍSQUES O DOCUMENTALS
5.21 Entrades i sortides de documents
5.22 Fitxers temporals

SALVETATS
I- BLOC GENERAL
5.5 Tercers
II- BLOC DE MESURES FÍSQUES O DOCUMENTALS
5.18 Control d'accés
5.19 Registre d'accessos
IV-BLOC DE MESURES ORGANITZATIVES
5.23 Registre d'incidències

Barcelona, 24 de febrer de 2017.

Pere Ruiz Espinós

- Soci-