ACTUALITZACIÓ DELS SISTEMES DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ A LA FUNDACIÓ HOSPITAL SANT BERNABÉ DE BERGA

Estudiant:	MONTSERRAT MAGNET SABATA
Consultor:	ARSENIO TORTAJADA GALLEGO
Programa:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Centre:	UOC/Fundació Hospital Sant Bernabé de Berga
Data lliurament:	02/06/2019

MONTSERRAT MAGNET SABATA

FITXA DEL TREBALL FINAL

Títol del treball:	Actualització dels Sistemes de gestió de la seguretat de la informació a la Fundació Hospital Sant Bernabé de Berga
Nom de l'autor:	MONTSERRAT MAGNET SABATA
Nom del consultor:	ARSENIO TORTAJADA GALLEGO
Data de lliurament (mm/aaaa):	06/2019
Àrea del Treball Final:	Sistemes de gestió de la seguretat de la informació Universitat Oberta de Catalunya
Titulació:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball :

Aquest projecte s'emmarca en el desenvolupament del Màster Interuniversitari de les Tecnologies de la Informació i la Comunicació que te per objectiu la implantació d'un Pla de seguretat de la informació , SGSI, en un entorn real, en aquest cas La FUNDACIO HOSPITAL SANT BERNABÉ,fundació Pública de serveis que treballa per prestar assistència hospitalària a la comarca del Berguedà i gestiona també una residencio d'avis, la RESIDENCIA SANT BERNABÉ.

Al llarg de les fases de creació del pla director de seguretat s'anirà construint tota la base necessària per a la preparació de la certificació de la ISO/IEC 27001:2013

Primer es fa un anàlisi inicial de l'estat en que es troba la fundació respecte a la ISO/IEC 27002:2013 per tal de tindre una visió de l'estat actual i de on es vol arribar respecte al nivell d'adaptació a la norma.

Posteriorment s'elabora el sistema documental exigit per la ISO/IEC 27001:2013, la política de seguretat i la metodologia d'anàlisi de riscos

Després es realitza aquest anàlisi de riscos de l'organització. en aquest cas, seguint la metodologia Magerit. En aquest punt es realitza el inventari d'actius i la seva valoració. També s'enumeren les amenaces que poden afectar a aquests actius i el impacte que tindrien.

Una vegada fet aquest passos anteriors es defineixen una sèrie de projectes que han de permetre minimitzar l'impacta de les amenaces detectades i es valora el cost de la seva implantació.

Per últim, es realitza un anàlisi de compliment respecte la ISO/IEC 27002:2013 considerant que els projectes anterior han estat implantats.

Abstract (in English, 250 words or less):

This project is framed in the development of the Interuniversity Master's in Information and Communication Technology "MISTIC", which aims to implement an Information Security Plan, SGSI, in a real environment, in this case The FUNDACIO HOSPITAL SANT BERNABÉ, Public Services Foundation that works to provide hospital care in the Berguedà region and also manages a residence for the elderly, RESIDENCIA SANT BERNABÉ.

Throughout the phases of the creation of the security plan, the entire base necessary for the preparation of ISO / IEC 27001: 2013 certification will be built

First, an initial analysis of the state in which the foundation is found in relation to ISO / IEC 27002: 2013 in order to have a vision of the current state and where it is intended to reach the level of adaptation to the norm.

The documentary system required by ISO / IEC 27001: 2013 is subsequently developed, the security policy and the risk analysis methodology.

After this analysis of risks of the organization is carried out. in this case, following the Magerit methodology. At this point, the asset inventory and its valuation are carried out. Also listed are the threats that may affect these assets and the impact they would have.

Once this step is done, a series of projects are defined that should allow minimizing the impact of the threats detected and the cost of its implementation is valued.

Finally, an analysis of compliance with the ISO / IEC 27002: 2013 is carried out , considering that the previous projects have been implemented.

Paraules clau (entre 4 i 8):

SGSI, seguretat, TFM, ISO27001, ISO27002 , MISTIC ,

Índex

1. Introducció

1.1 Context i justificació del Treball

La Fundació Benèfica de l'Hospital de Sant Bernabé, és una Fundació Pública de serveis benèfics i té per objecte fonamental prestar assistència hospitalària als malalts pobres i o totes les altres persones que compleixin les condicions que reglamentàriament es determinin. Gestiona també una residència d'avis.

Té la consideració d'organisme municipal autònom.

Actualment la Fundació consta de 2 edificis, l'Hospital y la Residència situats a Berga, comarca del Berguedà.

La Fundació va passar una auditoria de seguretat i disposa d'un pla de seguretat, des de l'any 2011 però aquest any 2019 ha implementat una nova infraestructura de sistemes Hyperconvergent, s'ha construït un segon CPD i s'han actualitzat els firewalls, degut a tots aquest canvis i a la intenció de obtenir una certificació ISO 27001 fa necessari actualitzar i replantejar el Pla Director de seguretat.

Aquest treball es centrarà en actualitzar el Pla Director de seguretat de la Fundació Hospital sant Bernabé i la seva adequació a la normativa ISO 27001:2013.

1.2 Objectius del Treball

L'Objectiu d'aquest treball es redactar i porta a terme l'actualització del sistema de gestió de la seguretat de la informació, en endavant SGSI de la Fundació Hospital Sant Bernabé.

1.3 ENFOCAMENT I MÈTODE SEGUIT

L'enfocament del treball es farà seguint l'Esquema Nacional de Seguretat, en endavant ENS, Real Decreto 3/2010, de 8 de gener modificat pel Real Decreto 951/2015, de 23 de octubre,)per obtenir una política de seguretat i determinar els principis basics per protegir la informació electrònica.

Aquest decret regula una de les peces fonamentals que vertebren el que s'ha anomenat la Administració Electrònica: la seguretat dels sistemes d'informació de les

Administracions Públiques, seguretat entesa com el conjunt de principis bàsics i requisits mínims requerits per a una protecció adequada de la informació tractada i els serveis prestats per les entitats del sector públic del seu àmbit d'aplicació.

Es pretén seguir l'estàndard ISO 27001:2013 que especifica els requisits necessaris per establir, implantar, mantenir i millorar un sistema de gestió de la seguretat de la informació (SGSI) segons el conegut com "Cicle de Deming": PDCA - acrònim de Pla, Do, Check, Act (Planificar, Fer , Verificar, Actuar).

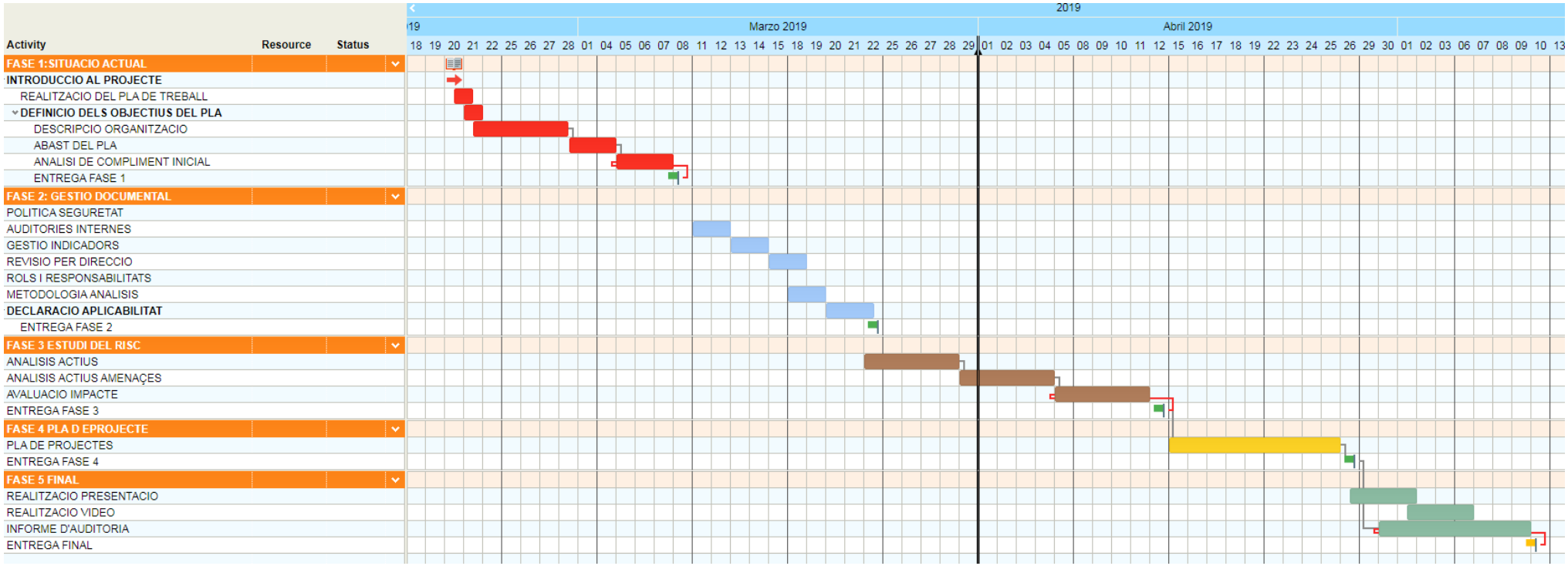
L'estratègia a seguir serà un estudi a fons de l'anterior Pla de Seguretat del 2011, de les modificacions tècniques que s'han dut a terme des de llavors i de les actualitzacions de les normatives existents i sota les que es va dissenyar l'anterior PLa.

- Revisió de tota la documentació anterior.
- Realització d'un nou pla de risc utilitzant el mètode MAGERIT amb els nous actius i els anteriors de la Fundació.
- Proposta d'un Pla d'auditoria a la direcció.
- Realització del projectes per millorar la seguretat segons el nou Pla.
- Valoració dels resultats.

1.4 PLANIFICACIÓ DEL TREBALL

Planificació temporal amb diagrama de Gant, les fites corresponent a les entregues de les PACS de la UOC

IL·LUSTRACIÓ 1 DIAGRAMA GANNT



1.5 BREU SUMARI DE PRODUCTES OBTINGUTS

1. Descripció detallada de la organització
2. Descripció dels sistemes d'informació
3. La Informació a la Fundació
4. Abast del pla director de Seguretat
5. Anàlisi de compliment inicial
6. Política de Seguretat
7. Procediment d'Auditories Internes
8. Gestió d'Indicadors
9. Procediment de Revisió per Direcció
10. Gestió de Rols i Responsabilitats
11. Metodologia de Anàlisis de Riscos
12. Declaració de Aplicabilitat
13. Analisis de Riscos
14. Pla de Projectes
15. Informe d'auditoria

2. Desenvolupament del TFM

2.1 PRIMERA FASE: SITUACIÓ ACTUAL

Contextualització, objectius i anàlisi de compliment

2.1.1DESCRIPCIÓ DETALLADA DE LA ORGANITZACIÓ

En aquest document es descriu La Fundació Sant Bernabé sobre la que es fa el treball.

Els seus orígens, l'evolució, la Governança, les xifres de recursos humans, de recursos estructurals i econòmics,l'entorn geogràfic i els serveis que ofereix.

Actualment la Fundació consta de 2 edificis, l'Hospital y la Residència situats a Berga, comarca del Berguedà.

L'Hospital ofereix serveis ambulatoris, d'hospitalització i sociosanitaris.

La Residència ofereix serveis de: Residència assistida, Acolliment Diürn, Programa Descans, Gent Gran a Casa, Serveis d'Atenció Domiciliària i d'Ajudes Tècniques.
Per últim s'inserta el Marc Normatiu de la Fundació.

Annexa 1

2.1.2 DESCRIPCIÓ DELS SISTEMES D'INFORMACIÓ

Es descriu el departament de Sistemes d'informació, tecnologia de la informació i comunicacions de la Fundació Hospital Sant Bernabé.

Aquest departament gestiona i dona suport als sistemes d'informació a les tecnologies de la informació i a la comunicació tan a l'Hospital Sant Bernabé com a la Residencia Sant Bernabé.

Es descriu la infraestructura tecnològica de la Fundació:

CPD's, Servidors físics i virtuals,cabines de emmagatzematge , elements de xarxa, impressores, ordinadors clients, telèfons mòbils, aparells de electromedicina, routers, firewalls.

Les Xarxes i el programari.

Annexa2

2.1.3 LA INFORMACIÓ A LA FUNDACIÓ

Aquest apartat intenta descriure la informació amb la que es treballa a la Fundació, la que és mes rellevant, tan a nivell de treball com a nivell de seguretat i la documentació que ja existeix sobre la organització de la seguretat, part del text es copia literal de documents existents a la Fundació.

Tipus d'informació

La informació amb que es treballa a la fundació conte un gran volum da dades que podríem classificar de varies maneres:

Dades de Pacients

Dades de Pacients, administratives i sanitàries englobades en la Historia clínica del pacient i en els programes SAVAC a l'hospital i Aegerus a la Residencia.

Dades del personal

Dades del personal (treballadors de la fundació), administratives i de salut que es troben en el programa DENARIO i que utilitza el departament de recursos Humans i Salut Laboral, com contractes, currículums ..

Dades de la Fundació

Dades de la Fundació com, documents legals, documents de compres i adquisicions, documents de expedients , factures, albarans, ...en el departament de Comptabilitat,compres, secretaria tècnica..

Bases de dades

Es llisten les bases de dades amb informació rellevant i que son les que cal protegir millor.

S'estudia la informació existent sobre seguretat a la Fundació.

Annexa 3

2.1.4 ABAST SGSI

Objectiu, abast i usuaris

L'objectiu d'aquest document és definir clarament els límits del Sistema de gestió de seguretat de la informació (SGSI) en La Fundació Hospital Sant Bernabé.

Aquest document s'aplica a tota la documentació i activitats dins del SGSI.

Els usuaris d'aquest document són els membres de la direcció de La Fundació Hospital Sant Bernabé, els membres de l'equip del projecte que implementa l'SGSI i el comitè de seguretat de la Fundació.

L'organització necessita definir els límits del SGSI per decidir quina informació vol protegir. Aquest tipus d'informació ha de ser protegida independentment de si a més és emmagatzemada, processada o transferida dins o fora de l'abast del SGSI.

El fet que determinada informació estigui disponible fora de l'abast no vol dir que no se li aplicaran les mesures de seguretat; això només implica que la responsabilitat per l'aplicació de les mesures de seguretat seran transferides a un tercer que administri aquesta informació.

Annexa 4

2.1.5 ANÀLISI DE COMPLIMENT INICIAL

En aquest apartat es realitza un anàlisi gap (Anàlisi diferencial) de controls implantats vs. controls necessaris, en relació amb la norma internacional ISO / IEC 27002, que desenvolupa un Codi de Bones Pràctiques per a la Gestió de la Seguretat de la Informació.

Primerament s'ha fet un anàlisis de aplicabilitat, per saber quins controls s'han d'analitzar i quins no.

Una vegada analitzada la informació de la Fundació I la seguretat que la protegeix, podem veure que :

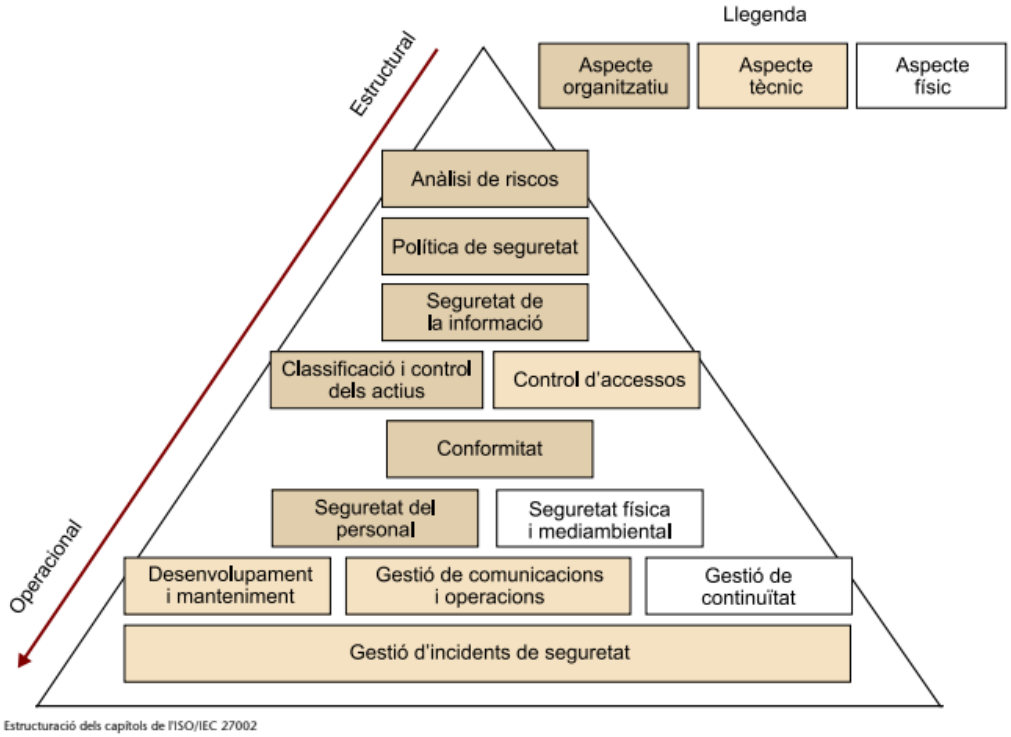
El nivell de maduresa mes alt el trobem en la Gestió d'incidents de seguretat, en la gestió de continuïtat del negoci i seguretat física i ambiental, degut a que la Política de seguretat fa temps que esta implementada (des de el 2011), que esta també auditada cada dos anys I adaptada a la RGPD i que existeix la figura del comitè de seguretat i del DPD, Delegat de protecció de dades (Sr. Roc mas, ADVOCAT).

Hi ha registre d'incidències de seguretat i estan protegits els accessos a la informació.

Falta en concret revisar tots els aspectes que han variat des de el 2016, sobretot el canvi que ha representat el pas a una arquitectura de sistemes hyperconvergent , la posada en funcionament del segon CPD , i el canvi de firewall.

Annexa 5

2.2 SEGONA FASE:
SISTEMA DE GESTIÓ DOCUMENTAL



IL·LUSTRACIÓ 2ISO 27002 CAPÍTOLS

2.2.1 POLÍTICA DE SEGURETAT

La política de seguretat és un document d'alt nivell que denota el compromís de la gerència amb la seguretat de la informació. Conté la definició de la seguretat de la informació des del punt de vista de l' entitat.

S'ha de tenir una normativa comuna de seguretat que reguli les línies mestres sobre la manera de treballar de tota l'organització en matèria de seguretat.

Tot el personal implicat en l'abast del SGSI ha de complir les polítiques de seguretat de la informació definides per l'organització, i han de ser revisades periòdicament.

En aquest cas també es llista a part d'una política general per la Fundació , tota la normativa que ja existeix documentada.

Annexa 6

2.2.2PROCEDIMENT D'AUDITORIES INTERNES

El procés d'auditoria, de manera general, és l'aplicació d'una revisió sistemàtica del compliment d'uns criteris d'auditoria.

La independència de l'activitat auditada es una de les bases per que una auditoria sigui imparcial i objectiva.

El principi d'independència exigeix que els auditors, no tinguin influencies sobre la activitat auditada.

En les auditories de primera part (internes) el destinatari final dels resultats del treball és la mateixa organització , l'equip auditor pot ser intern per auto avaluar l'activitat o extern.

El propòsit de l'auditoria és verificar que l'entitat auditada treballa d'acord amb la normativa interna i externa

En base a la implantació de un procés continu de millora, conegut com a cicle Deming o Shewart composat per 4 processos que es van repetint iterativa ment:

- Planificar (que volem fer i com)
- Implementar (el que planifiquem)
- Comprovar (analitzar el funcionament)

- Actuar (segons la revisió que fem)

les auditories no son independents les unes de les altres si no que es complementen. La repetició d'un cicle ha de donar lloc a identificar i implementar les possible millores detectades.

Annexa 7

2.2.3GESTIÓ D'INDICADORS

L'aplicació de la norma ISO 27001 requereix seleccionar un conjunt d'objectius

de control per veure si s'assoleixen els criteris d'acceptació de risc i donar així compliment als objectius del procés de millora contínua.

lA ISO 27004 (2016) E ens indica que mesurar (p 6.3):

processos, activitats, controls i grups de controls.

També ens indica Tipus de mesures (p 7)

Generalitats (7.1)

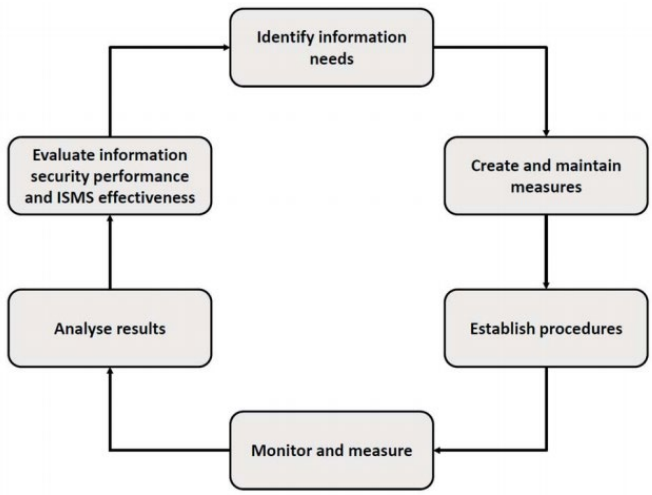
a) les mesures de rendiment: mesures que expressen els resultats previstos en termes de les característiques

b) mesures d'eficàcia: mesures que expressen el sentit que la realització de les activitats previstes
Les mesures d'acompliment (p 7.2)

Les mesures de rendiment es poden utilitzar per demostrar el progrés en la implementació de processos de SGSI, les activitats associades s'han realitzat amb la intenció resultats assolits, les mesures de rendiment haurien referir-se a les activitats de SGSI.

Eficàcia de les mesures (7.3)

Les mesures d'eficàcia s"utilitzen per descriure l'eficàcia i l'impacte que les realitzacions dels processos del pla SGSI, tractament del risc i els controls tenen en la informació de l'organització



processos i controls relacionats
IL·LUSTRACIÓ 3 ISO 2004

Annexa 8

2.2.4PROCEDIMENT DE REVISIÓ PER DIRECCIÓ

La Direcció de l'Organització ha de revisar a intervals planificats les qüestions més importants que han anat passant en relació al Sistema de Gestió de Seguretat de la Informació.
Per aquesta revisió, la ISO/IEC 27001 defineix, tant els punts d'entrada, com els punts de sortida que han d'obtenir-se.

ISO 27001: 2013 punt 9.3

La revisió per la direcció ha d'incloure consideracions sobre:

a) l'estat de les accions de anteriors revisions per la direcció;

b) els canvis en les qüestions externes i internes que siguin pertinents al sistema de gestió de la seguretat de la informació;

c) la informació sobre el comportament de la seguretat de la informació, incloses les tendències relatives a:

1) no conformitats i accions correctives,

2) seguiment i resultats dels mesuraments,

3) resultats d'auditoria, i

4) el compliment dels objectius de seguretat de la informació,

d) els comentaris provinents de les parts interessades;

e) els resultats de l'apreciació dels riscos i l'estat del pla de tractament de riscos; i

f) les oportunitats de millora contínua.

Els elements de sortida de la revisió per la direcció han d'incloure les decisions relacionades amb les oportunitats de millora contínua i qualsevol necessitat de canvi en el sistema de gestió de la seguretat de la informació.

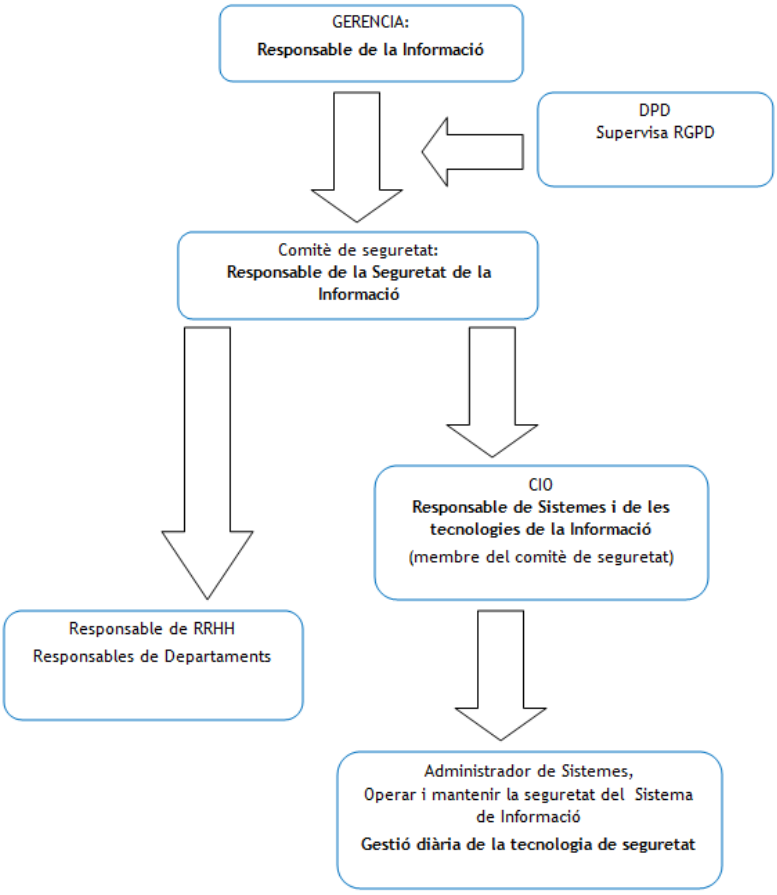
L'organització ha de conservar informació documentada com evidència dels resultats de les revisions per la direcció.

Annexa 9

2.2.5 GESTIÓ DE ROLS I RESPONSABILITATS

La Política de Seguretat, segons requereix l'Annex II de l'ENS en la seva secció 3.1, ha d'identificar uns clars responsables per vetllar pel seu compliment i ser coneguda per tots els membres de l'organització administrativa.

S'estableixen els rols en l'organització relacionats amb la Seguretat de la Informació que es descriuen en l'annexa 10



IL·LUSTRACIÓ 4 JERARQUIA SEGURETAT

Annexa 10

2.2.6 METODOLOGIA DE ANÀLISIS DE RISCOS

Hi ha diverses aproximacions al problema d'analitzar els riscos suportats pels sistemes TIC: guies informals, aproximacions metòdiques i eines de suport.

Totes busquen objectivar l'anàlisi de riscos per a saber com de segurs (o insegurs) són els sistemes.

El gran repte de totes aquestes aproximacions és la complexitat del problema ,complexitat en el sentit que hi ha molts elements que considerar i que, si no s'és rigorós, les conclusions seran poc fiables. És per això que utilitzarem MAGERIT.

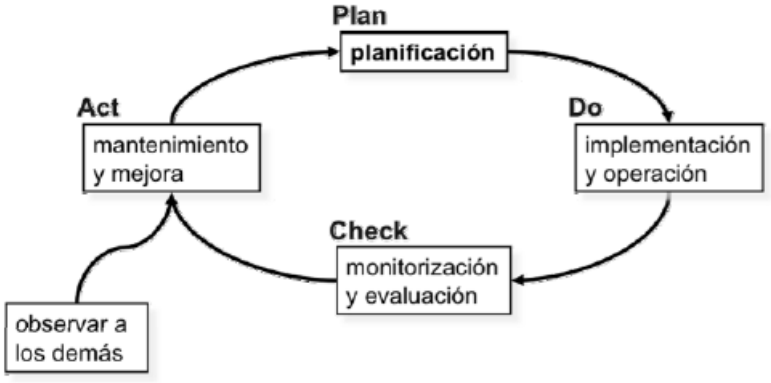
Magerit persegueix una aproximació metòdica que no deixi lloc a la improvisació, ni depèn de l'arbitrarietat de l'analista.

MAGERIT V3

Són les sigles de Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'Informació de l' Administracions, aquest mètode cobreix la fase AGR (Anàlisi i Gestió de Riscos).

És elaborada pel Consell Superior d'Administració Electrònica, com a resposta a la percepció que l'Administració, i, en general, tota la societat, depenen de forma creixent de les tecnologies de la informació per al compliment de la seva missió. Consisteix en investigar els riscos que suporten els Sistemes d'Informació i per recomanar les mesures apropiades que s'haurien d'adoptar per controlar aquests riscos.

L'anàlisi de riscos és part de les activitats de planificació, on es prenen decisions de tractament. Aquestes decisions es materialitzen en l'etapa d'implantació, on convé desplegar elements que permetin la monitorització de les mesures desplegades per poder avaluar l'efectivitat de les mateixes i actuar en conseqüència, dins d'un cercle d'excel·lència o millora contínua.



IL·LUSTRACIÓ 5/ CICLE DENNING

Annexa 11

2.2.7 DECLARACIÓ DE APLICABILITAT

Document que inclou tots els controls de Seguretat establerts a la Organització, amb el detall de la seva aplicabilitat, estat i documentació relacionada.

ISO 27001 apartat 6.1.3 d)

elaborar una “Declaración de Aplicabilidad” que contenga:

- los controles necesarios [véase 6.1.3 b) y c)];
- la justificación de las inclusiones;
- si los controles necesarios están implementados o no; y
- la justificación de las exclusiones de cualquiera de los controles del anexo A.

La norma ISO 27002: 200.517 (anteriorment 17799): "Codi de bones pràctiques per a la gestió de la seguretat de la informació "desenvolupa l'Annex A de la norma ISO 27001 proporcionant assessorament per a la seva implantació.

Es defineix control (sinònim de salvaguarda o contramesura) com:

"Mitjà de gestió del risc que inclou polítiques, procediments,directrius, pràctiques o estructures de l'organització que poden ser de naturalesa administrativa, tècnica, de gestió i legal ".

Es presenta un conjunt de 133 controls, agrupats en 39 objectius de control que ho fan, al seu torn, en 11 dominis. A la pràctica les organitzacions podren excloure alguns o afegir altres sempre que es justifiqui adequadament. el document que contempla la totalitat de controls seleccionats i la seva justificació s'anomena Declaració de Aplicabilitat (SOA).

Annexa 12

2.3 TERCERA FASE: ANÁLISIS DE RISCOS

El centre criptológic nacional disposa d'una eina de anàlisis del risc desenvolupada per ells mateixos anomenada **PILAR**, he demanat una llicencia per utilitzar-la en aquest projecte.

Les eines EAR suporten l'anàlisi i la gestió de riscos d'un sistema d'informació seguint la metodologia Magerit explicada en un annexa anterior.

L'anàlisi de riscos es centra en els incidents que poden causar un perjudici a la informació i els serveis de l'organització, proporciona informació per a decidir sobre l'assignació de recursos, ja siguin tècnics o d'altre tipus, per protegir organització.

L'anàlisi de riscos requereix un enfocament metòdic:

- identificar el valor que cal protegir,
- Identificar els elements del sistema que suporten aquest valor,aquells on els atacs poden fer mal
- establir mesures de seguretat per protegir-nos contra els atacs
- estimar indicadors de la posició de risc per ajudar els que tenen de prendre decisions.

Els actius estan exposats a amenaces que, quan es materialitzen, degraden l'actiu, produint un impacte. Si estimem la freqüència amb què es materialitzen les amenaces, podem deduir el risc a què està exposat el sistema. Degradació i freqüència qualifiquen la vulnerabilitat del sistema.

El gestor del sistema d'informació disposa de salvaguardes, que o bé redueixen la freqüència d'ocurrència, o bé redueixen o limiten l'impacte. Depenent del grau d'implantació d'aquestes salvaguardes, el sistema passa a una nova estimació de risc que s'anomena risc residual.

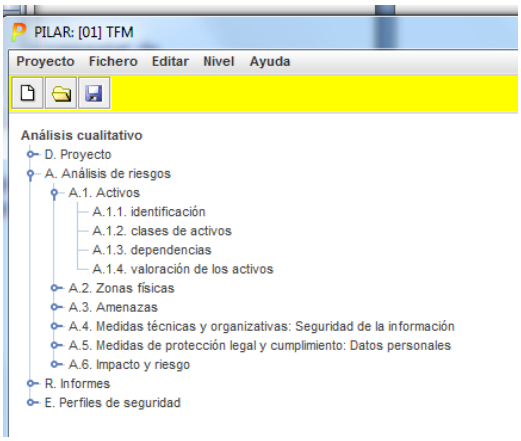
PILAR disposa d'una biblioteca estàndard de propòsit general, i és capaç de realitzar qualificacions de seguretat respecte de normes àmpliament conegudes com són:

ISO / IEC 27002 (2005, 2013) - Codi de bones pràctiques per a la Gestió de la Seguretat de la Informació

ENS - Esquema Nacional de Seguretat

El primer que ha calgut fer es llistar i agrupar els actius :

TASCA A.1



[B] Actius essencials

[PROC] Procediments (inclouen un o mes serveis interns)

He inclòs també com a procés essencial les solucions de contingència implantades, com a molt important per nosaltres es el Procés de Historia clínica que conte totes les dades dels nostres clients (pacients) , la Gestió de recursos humans es un altre procés essencial i la gestió administrativa.

[DOCS]Documents, Informació

He considerat informació valuosa i a protegir els inventaris, les copies de maquines virtuals, les credencials, les configuracions, els llistats que utilitzem en cas de contingència (cal que tinguin una disponibilitat i integritat elevadíssima), els documents dels usuaris i les llicencies (ni han que tenen molt valor econòmic com la de data-center de Microsoft).

[BD Bases de dades

Contenen les dades essencials de l'organització, en aquest cas la de Oracle (Savac)inclou les dades dels pacients, les del PACS inclou les imatges radiològiques, les de Denario contenen les dades de recursos humans les de Dimoni de comptabilitats etc..que son bases de dades SQL.

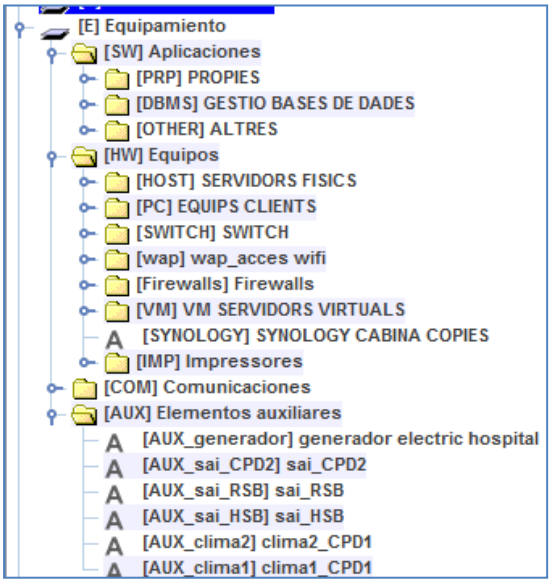
[S] Serveis

Hi he inclòs els serveis de cada cas de contingència ,

- Contingència 1.No funciona His, savac
- Contingència 2.No hi ha energia elèctrica i cal comptar amb el generador
- Contingència 3.No hi ha xarxa LAN interna o part d'ella
- Contingència 4.Hi ha hagut pèrdua d'informació

[E] Equipament

Inclou les aplicacions, que he distingit entre les de producció pròpia, els gestors de les bases de dades i la resta.



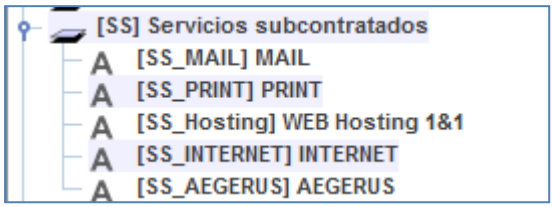
En els equips he distingit els Host, els clients per àrees, els switch, els wap, els firewalls, les maquines virtuals , la cabina de copies i les impressores.

Dins de comunicacions hi trobarem les xarxes, les LAN de residencia i hospital , el Nus Sanitari, i els internets.

[AUX] Elements auxiliars

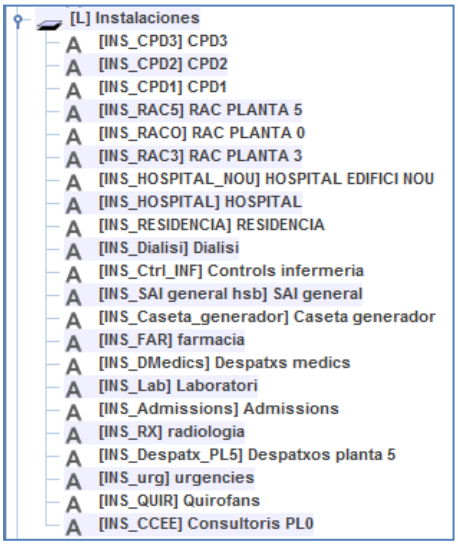
Com element auxiliar tenim un generador elèctric, els SAIS i els Climes del CPD.

[SS] serveis subcontractats



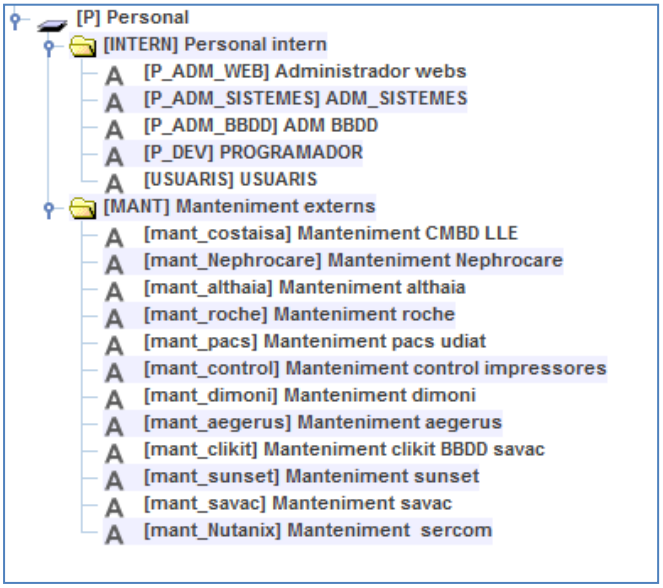
Els serveis que tenim subcontractats

[L] Instal·lacions



S'han agrupat per àrees de interès de seguretat, per exemple els diferents CPD, les àrees de urgències , de radiologia , els armaris de racks de switchs, centrals d'infermeria , despatxos de consulta mèdica entre altres.

[P] Personal



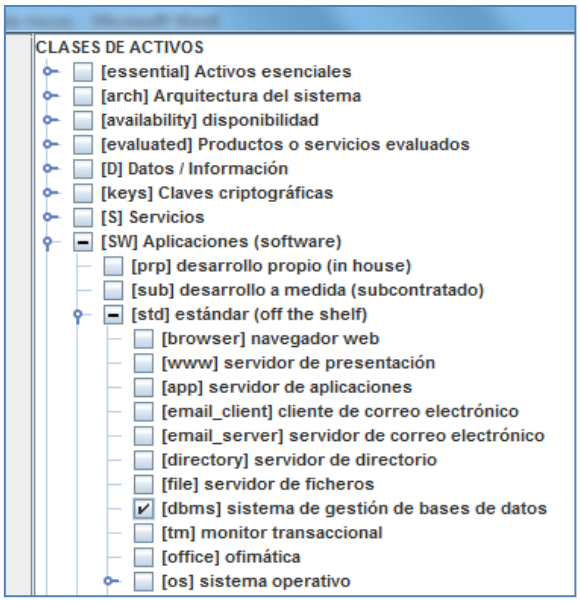
He distingit entre personal intern i el personal de manteniments externs, necessaris en casos d'averies, canvis configuracions etc..

TASCA A.1.2

Classes de actius

A cada actiu se li ha signat una classe o mes d'una.

Exemple: DBMA_Cache es una aplicació DBMS de gestió de base de dades



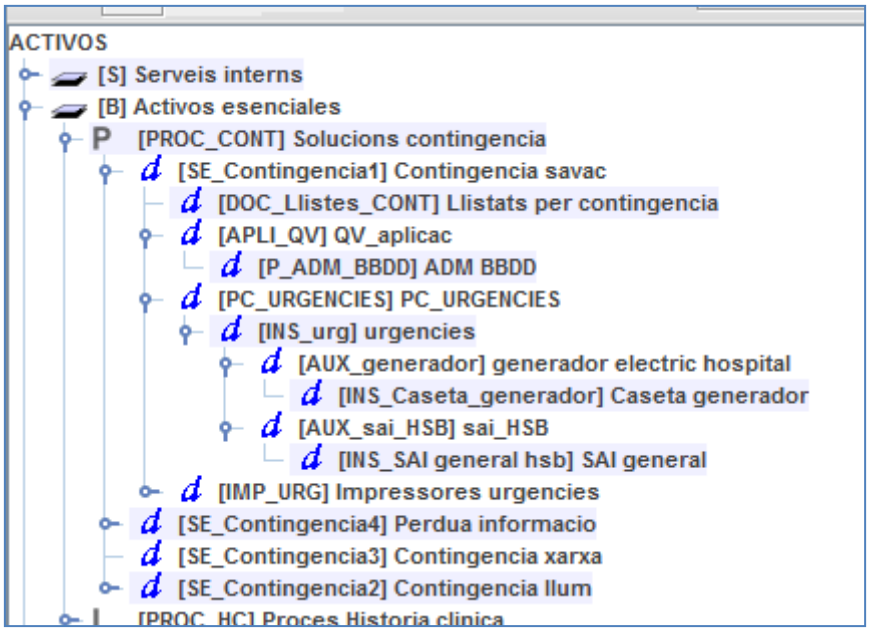
TASCA A 1.3 Dependencies

En aquest apartat he valorat les dependencies entre actius.

Per fer aquestes dependencies he utilitzat aquestes formules :

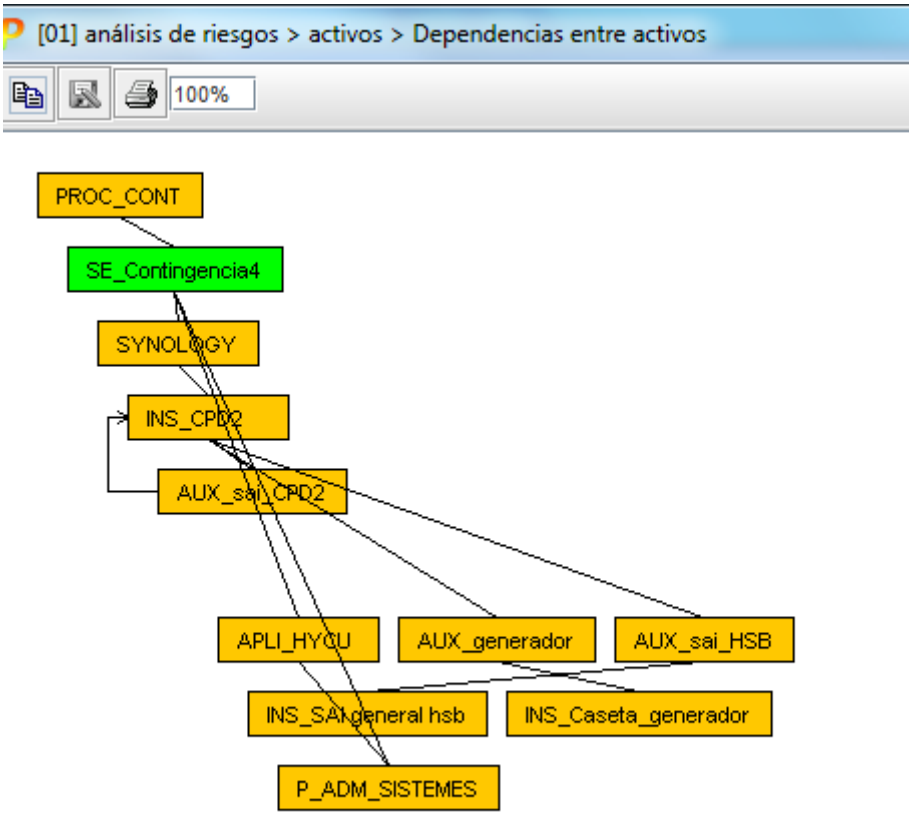
- Els processos depenen de serveis.
- Les bases de dades depenen del administrador de sistemes, del manteniment extern de l'aplicació, i del programa gestor.
- Les aplicacions del seu administrador intern i l'equip que les sustenta.
- Els equips, del lloc on estan físicament.
- Les maquines virtuals dels seu host.
- Les comunicacions dels aparells que les suporten.
- Els serveis de: les aplicacions del personal que les gestiona, de les BBDD en algun cas etc..

HI ha algun cas especial com els CPD que depenen dels SAIS, dels Climes, del generador extern...etc

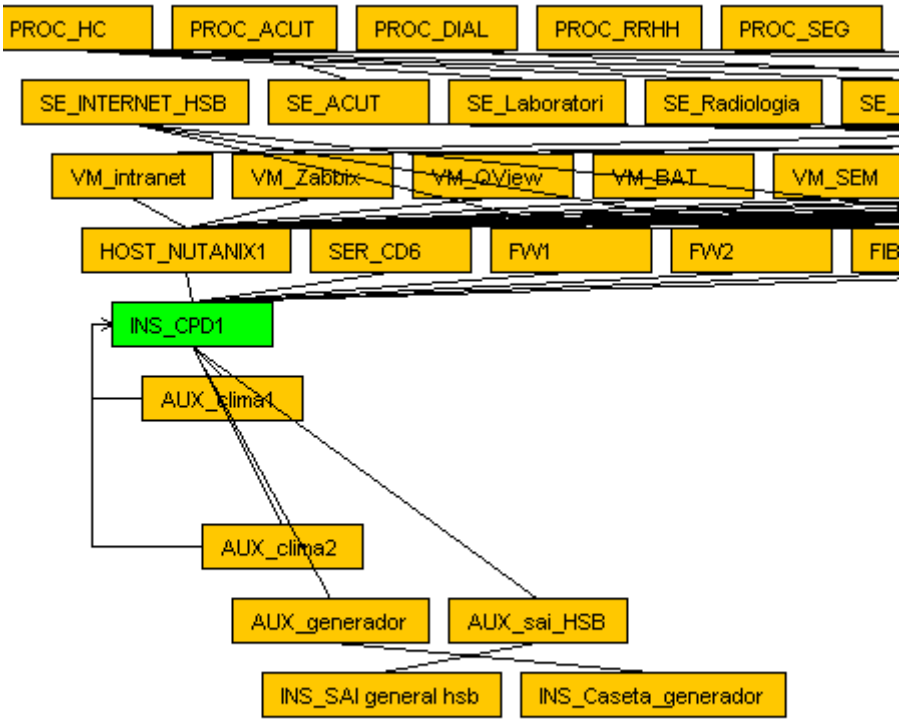


En aquest punt el programa permet ja crear alguns gràfics.

Procés de dependencies del servei de contingència (color verd), en cas de pèrdua d'informació (per sobre podem veure el Procés on esta contingut el servei)

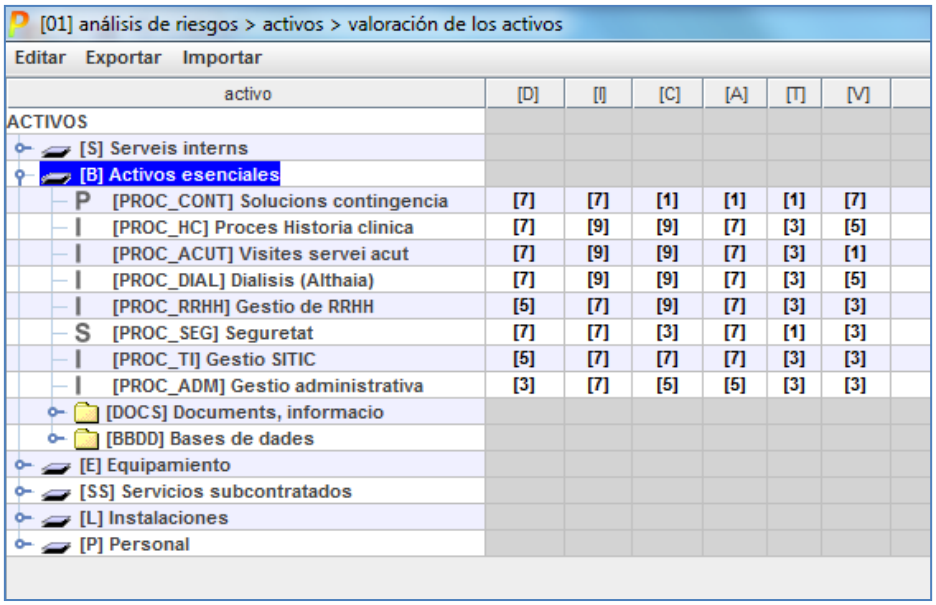


gràfic de dependencies del CPD1 (color verd)



TASCA A 1.4

Valoració dels actius

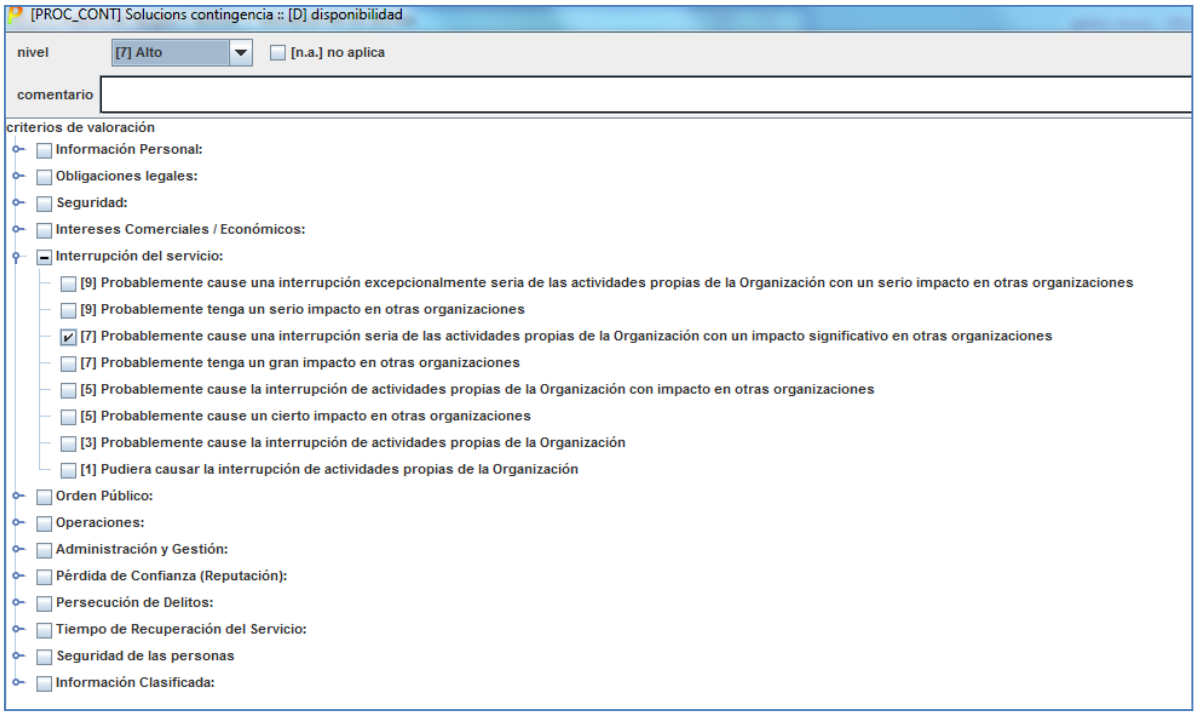


activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS						
[S] Serveis interns						
[B] Activos esenciales						
P [PROC_CONT] Solucions contingencia	[7]	[7]	[1]	[1]	[1]	[7]
[PROC_HC] Proces Historia clinica	[7]	[9]	[9]	[7]	[3]	[5]
[PROC_ACUT] Visites servei acut	[7]	[9]	[9]	[7]	[3]	[1]
[PROC_DIAL] Dialisis (Althaia)	[7]	[9]	[9]	[7]	[3]	[5]
[PROC_RRHH] Gestio de RRHH	[5]	[7]	[9]	[7]	[3]	[3]
S [PROC_SEG] Seguretat	[7]	[7]	[3]	[7]	[1]	[3]
[PROC_TI] Gestio SITIC	[5]	[7]	[7]	[7]	[3]	[3]
[PROC_ADM] Gestio administrativa	[3]	[7]	[5]	[5]	[3]	[3]
[DOCS] Documents, informacio						
[BBDD] Bases de dades						
[E] Equipamiento						
[SS] Servicios subcontratados						
[L] Instalaciones						
[P] Personal						

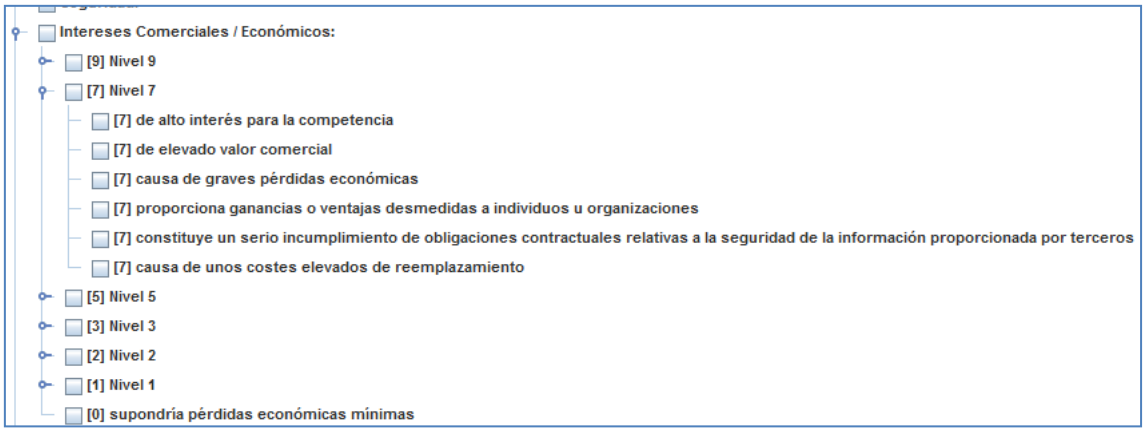
Aquesta tasca ha sigut especialment llarga per que s'ha de valorar de cada actiu, la [D] disponibilitat, la [I] integritat, [C]Confidencialitat, [T] traçabilitat, [V]el valor , la [DP] dades personals

Per fer aquestes valoracions, el programa dona uns ***items*** que cal estudiar i puntuar(en aquest cas en aplica ISO 27001) :

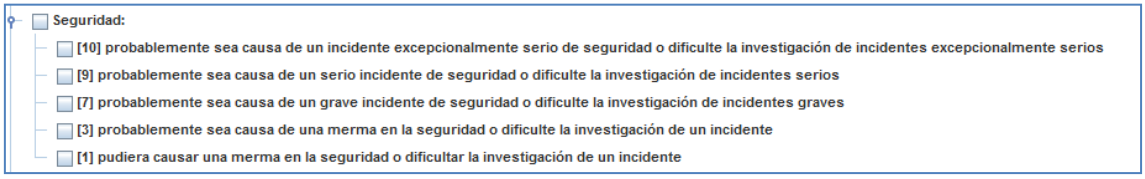
Ex. Interrupció del servei ,podria causar:



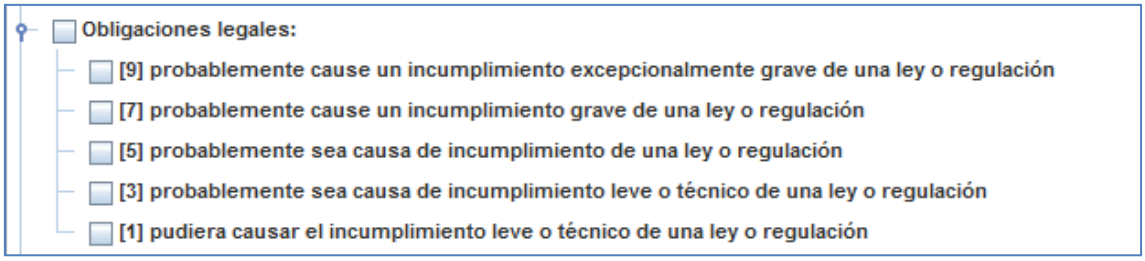
EX Interès comercial o econòmic



Seguretat



Obligacions legals



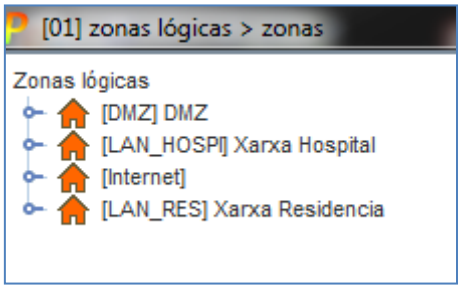
s'han valorat tots els actius per cada dimensió

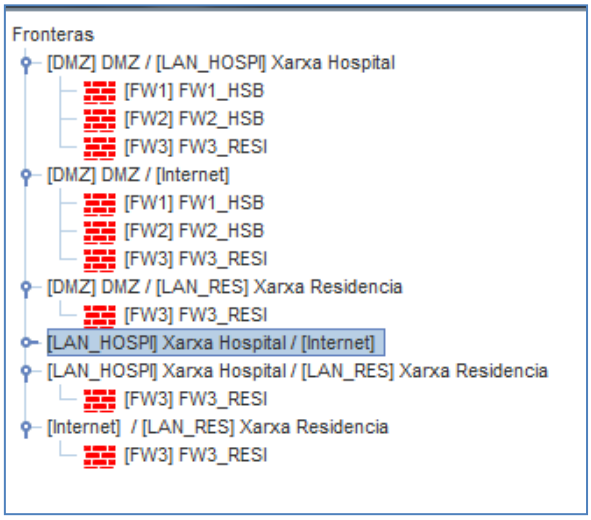
TASCA A 2 Zones

TASCA A 2 .1

Es poden organitzar zones al voltant de les fronteres o perímetres, diferenciant entre els actius que estàn a un costat i a l'altre.

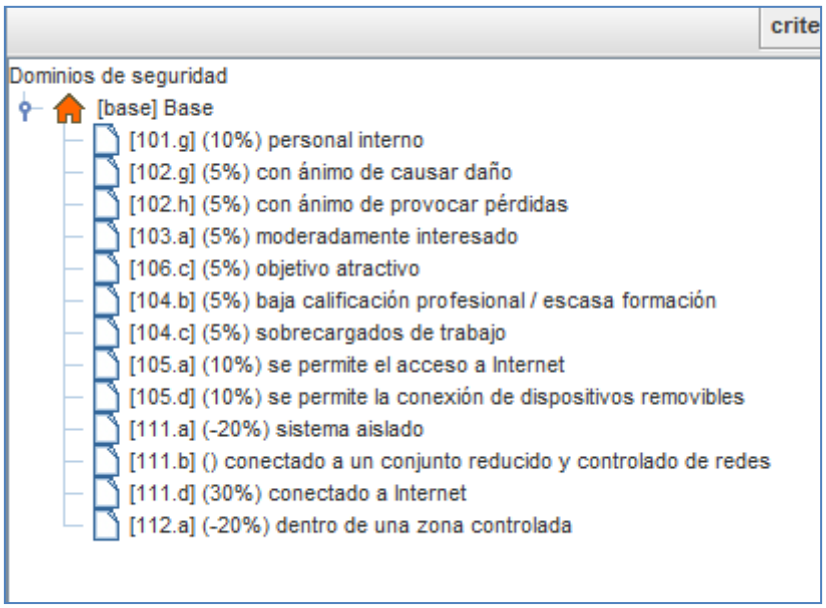
He organitzat veries zones, DMZ, Intranet, Xarxa Hospital i Xarxa residencia i les fronteres logiques entre elles que son els firewalls.





A 3.1 Factors agreujants i atenuants

Podem afegir factors que considerem que poden agreujar o atenuar les amenaces, en aquest cas he considerat els següents :

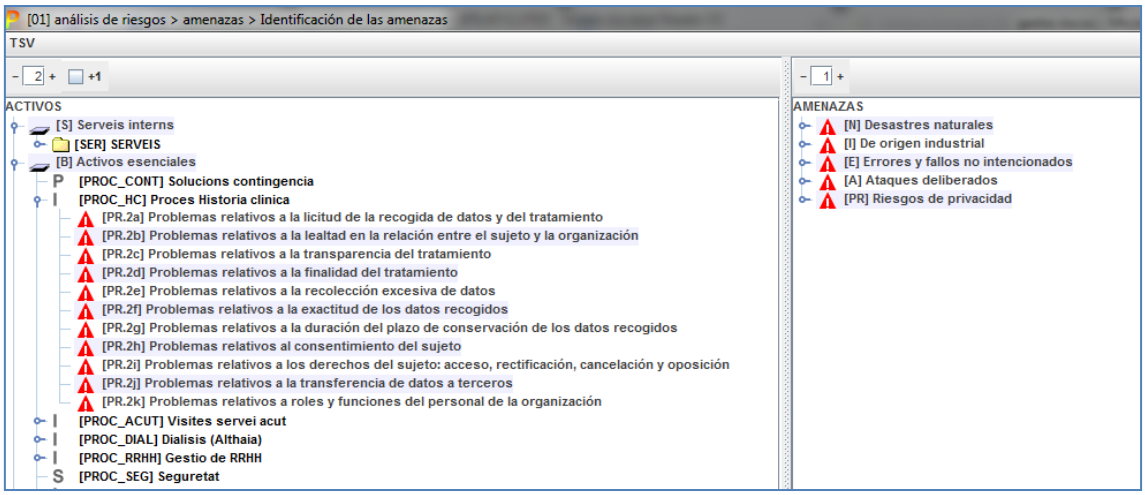


A 3.2 identificar les amenaces

El programa pot funcionar de 3 maneres,

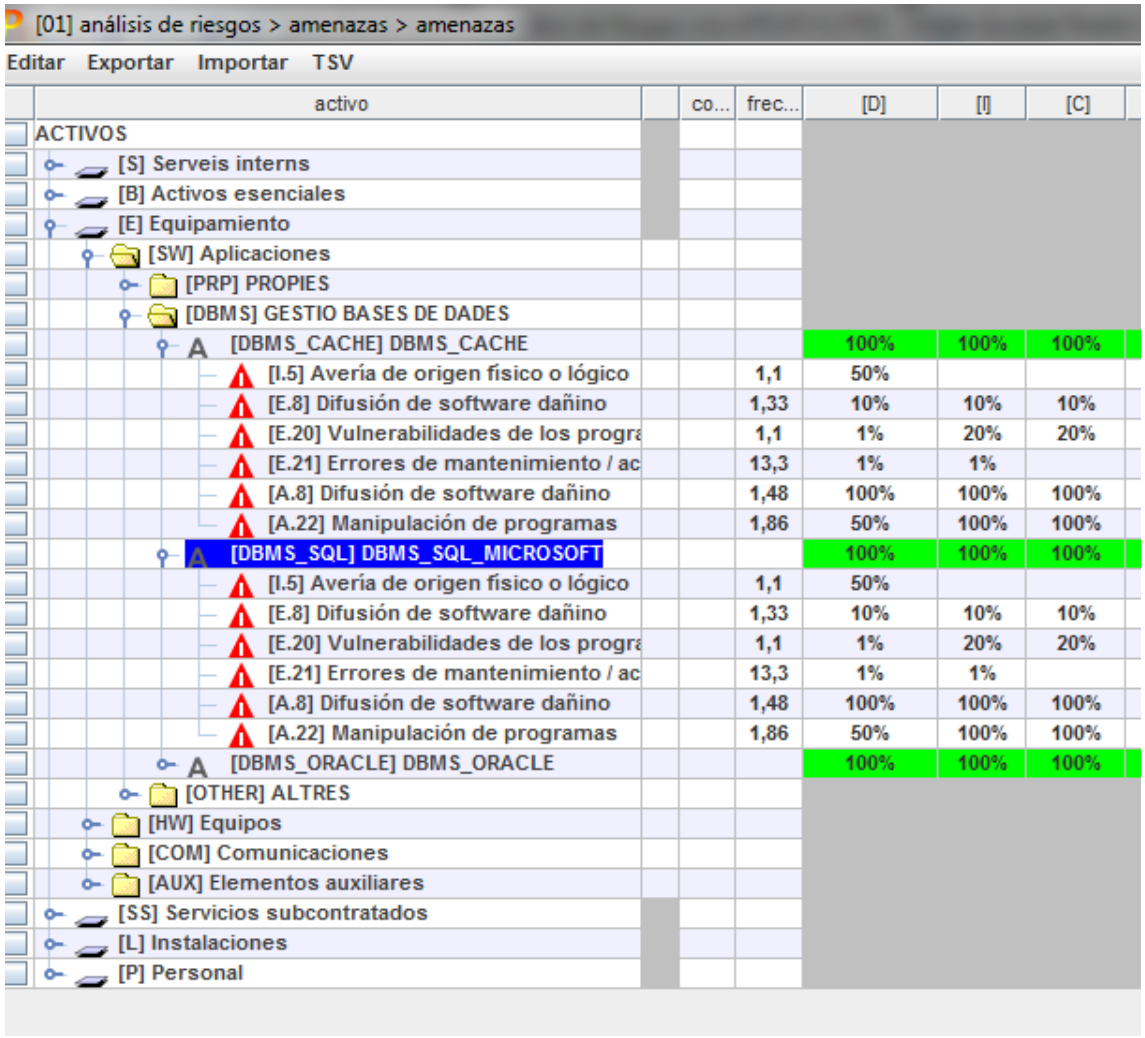
- automàtic , ell decideix les amenaces segons el tipus de actiu.
- mixta , ell decideix però es pot modificar.
- manual, s'han de assignar manualment.

en aquest cas jo he utilitzat la manera **mixta,** i en algun cas he afegit o tret amenaces



A 3.3 valoració de les amenaces

Aquesta part el programa la calcula automàticament.



A 4.1 Valoració per fases

Aquesta fase ha sigut molt laboriosa per que demana valorar totes les salvaguardes que proposa automàticament, en nivell de maduresa entre

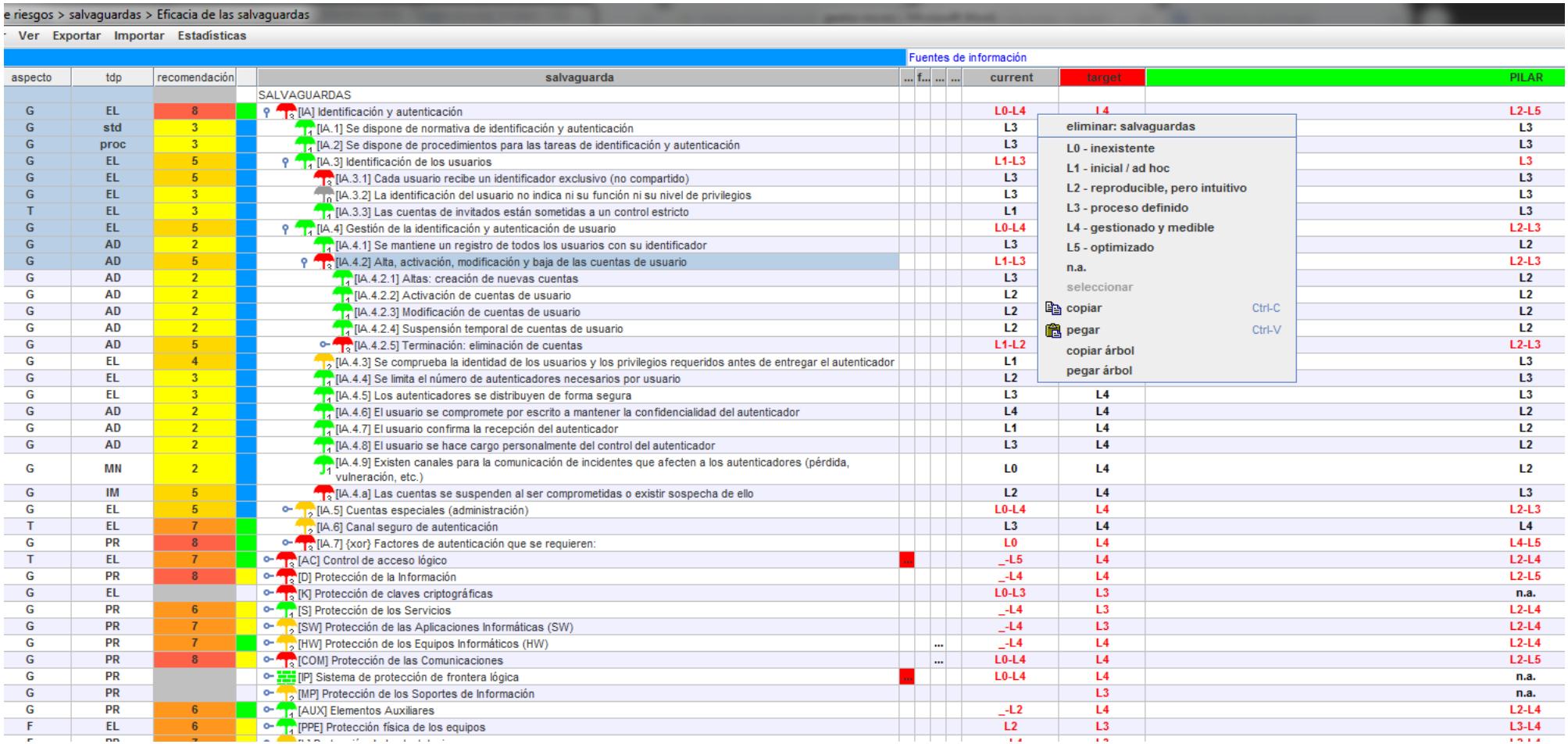
L0-L5.

He valorat 2 columnes

current -> on estem en aquest moment,

target -> on volem arribar ,

i la tercera columna PILAR, ens dona el nivell òptim que considera el programa que hauríem d'assolir.


e riesgos > salvaguardas > Eficacia de las salvaguardas
Ver
Exportar
Importar
Estadísticas
Fuentes de información
aspecto
tdp
recomendación
salvaguarda
current
target
PILAR
SALVAGUARDAS
[IA] Identificación y autenticación
[IA.1] Se dispone de normativa de identificación y autenticación
[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación
[IA.3] Identificación de los usuarios
[IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)
[IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios
[IA.3.3] Las cuentas de invitados están sometidas a un control estricto
[IA.4] Gestión de la identificación y autenticación de usuario
[IA.4.1] Se mantiene un registro de todos los usuarios con su identificador
[IA.4.2] Alta, activación, modificación y baja de las cuentas de usuario
[IA.4.2.1] Altas: creación de nuevas cuentas
[IA.4.2.2] Activación de cuentas de usuario
[IA.4.2.3] Modificación de cuentas de usuario
[IA.4.2.4] Suspensión temporal de cuentas de usuario
[IA.4.2.5] Terminación: eliminación de cuentas
[IA.4.3] Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador
[IA.4.4] Se limita el número de autenticadores necesarios por usuario
[IA.4.5] Los autenticadores se distribuyen de forma segura
[IA.4.6] El usuario se compromete por escrito a mantener la confidencialidad del autenticador
[IA.4.7] El usuario confirma la recepción del autenticador
[IA.4.8] El usuario se hace cargo personalmente del control del autenticador
[IA.4.9] Existen canales para la comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)
[IA.4.a] Las cuentas se suspenden al ser comprometidas o existir sospecha de ello
[IA.5] Cuentas especiales (administración)
[IA.6] Canal seguro de autenticación
[IA.7] {xor} Factores de autenticación que se requieren:
[AC] Control de acceso lógico
[D] Protección de la Información
[K] Protección de claves criptográficas
[S] Protección de los Servicios
[SW] Protección de las Aplicaciones Informáticas (SW)
[HW] Protección de los Equipos Informáticos (HW)
[COM] Protección de las Comunicaciones
[IP] Sistema de protección de frontera lógica
[MP] Protección de los Soportes de Información
[AUX] Elementos Auxiliares
[PPE] Protección física de los equipos
eliminar: salvaguardas
L0 - inexistente
L1 - inicial / ad hoc
L2 - reproducible, pero intuitivo
L3 - proceso definido
L4 - gestionado y medible
L5 - optimizado
n.a.
seleccionar
copiar Ctrl-C
pegar Ctrl-V
copiar árbol
pegar árbol

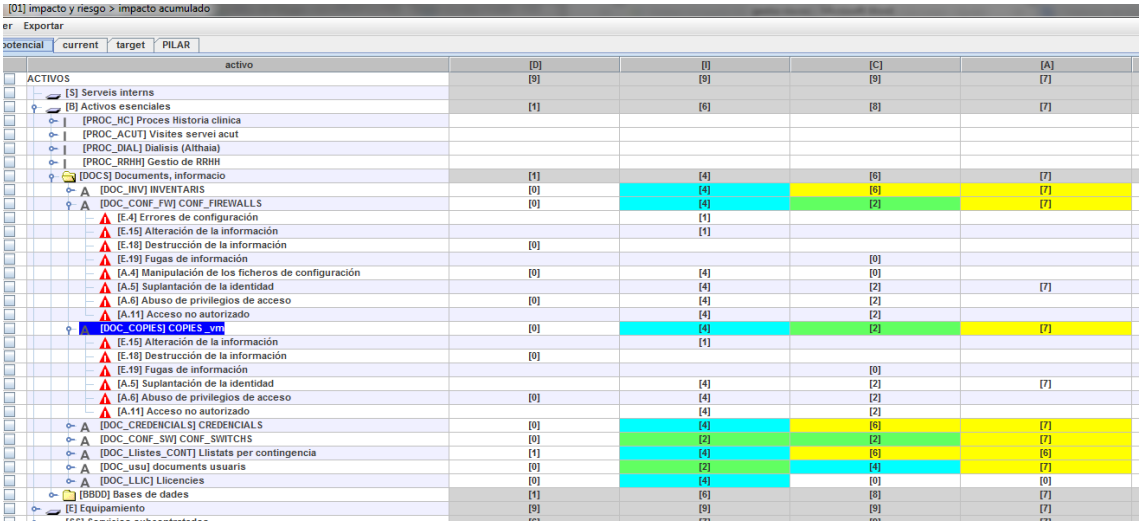
A 6. Impacta i risc

A partir d'aquí podem obtenir la valoració del risc i l'impacta.

Ens mostra:

- el risc potencial (sense salvaguardes),
- el risc corrent (aplicant les salvaguardes que tenim actuals) ,
- el target (seria una vegada haguéssim aplicat les salvaguardes al nivell que voldríem tenir)
- i el PILAR (aplicant la que ens recomana el programa).

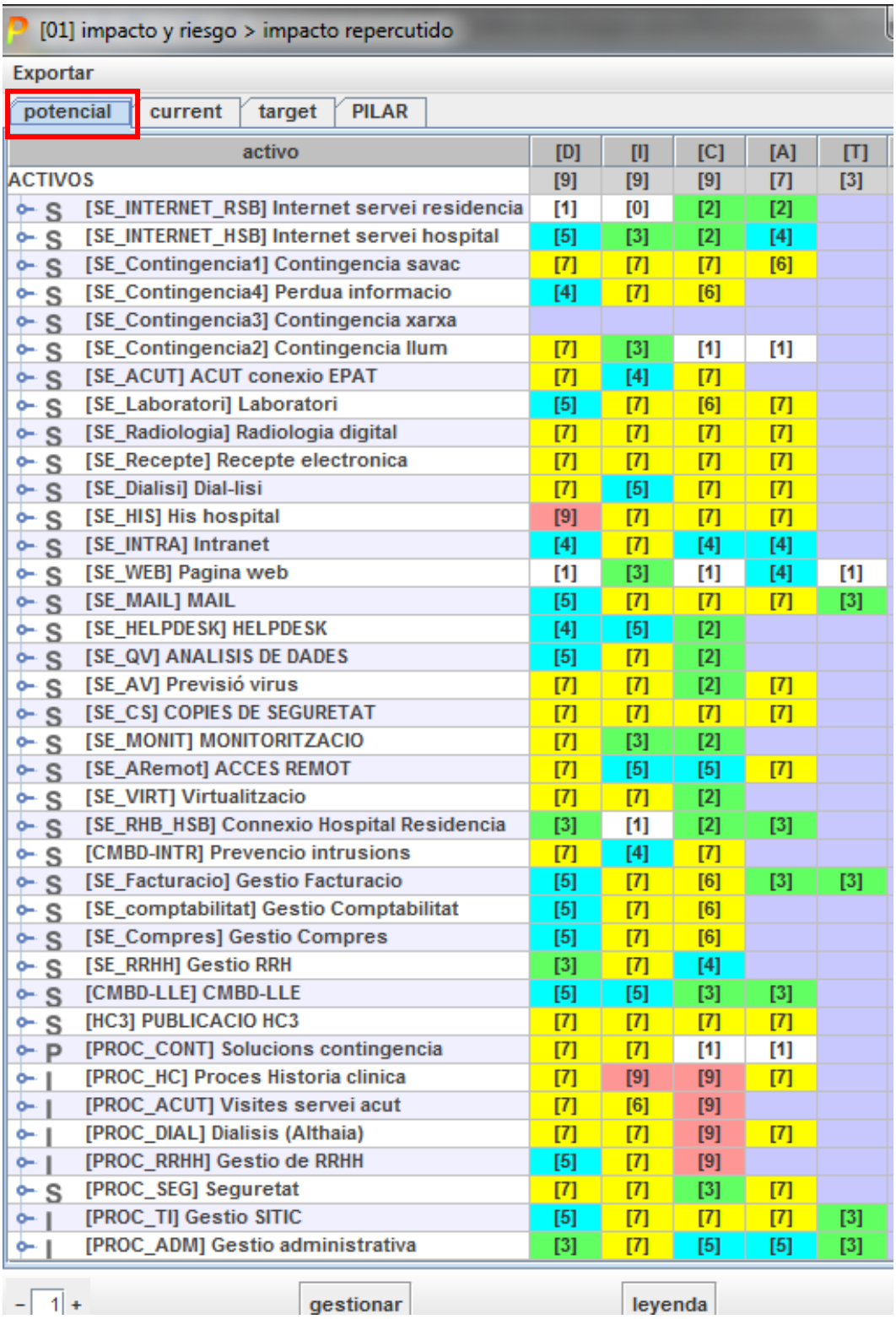
Diferents colors segons les dependencies de l'actiu



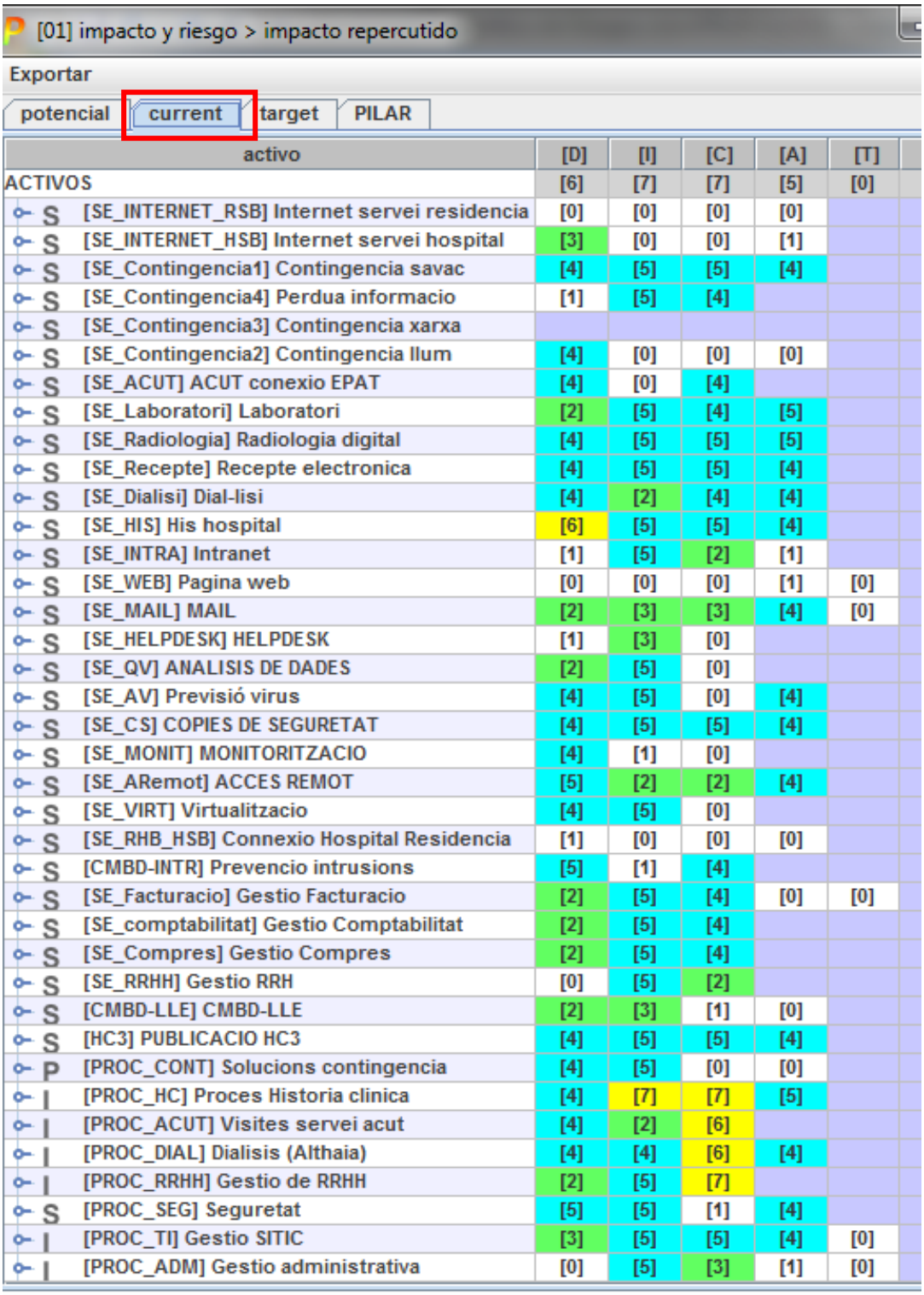
activo	[D]	[I]	[C]	[A]
ACTIVOS	[9]	[9]	[9]	[7]
[S] Serveis interns				
[B] Activos esenciales	[1]	[6]	[8]	[7]
[PROC_HC] Proces Historia clínica				
[PROC_ACUT] Visites servei acut				
[PROC_DIAL] Dialisis (Althaia)				
[PROC_RRHH] Gestio de RRHH				
[DOCS] Documents, informacio	[1]	[4]	[6]	[7]
[DOC_INV] INVENTARIS	[0]	[4]	[6]	[7]
[DOC_CONF_FW] CONF_FIREWALLS	[0]	[4]	[2]	[7]
[E.4] Errores de configuración		[1]		
[E.15] Alteración de la información		[1]		
[E.18] Destrucción de la información	[0]			
[E.19] Fugas de información			[0]	
[A.4] Manipulación de los ficheros de configuración	[0]	[4]	[0]	
[A.5] Suplantación de la identidad		[4]	[2]	[7]
[A.6] Abuso de privilegios de acceso	[0]	[4]	[2]	
[A.11] Acceso no autorizado		[4]	[2]	
[DOC_COPIES] COPIES_vm	[0]	[4]	[2]	[7]
[E.15] Alteración de la información		[1]		
[E.18] Destrucción de la información	[0]			
[E.19] Fugas de información			[0]	
[A.5] Suplantación de la identidad		[4]	[2]	[7]
[A.6] Abuso de privilegios de acceso	[0]	[4]	[2]	
[A.11] Acceso no autorizado		[4]	[2]	
[DOC_CREDENCIALS] CREDENCIALS	[0]	[4]	[6]	[7]
[DOC_CONF_SW] CONF_SWITCHS	[0]	[2]	[2]	[7]
[DOC_Llistes_CONT] Llistats per contingencia	[1]	[4]	[6]	[6]
[DOC_usu] documents usuaris	[0]	[2]	[4]	[7]
[DOC_LLIC] Llicencies	[0]	[4]	[0]	[0]
[BBDD] Bases de dades	[1]	[6]	[8]	[7]
[E] Equipamiento	[9]	[9]	[9]	[7]

A 6.2 Valors repercutits

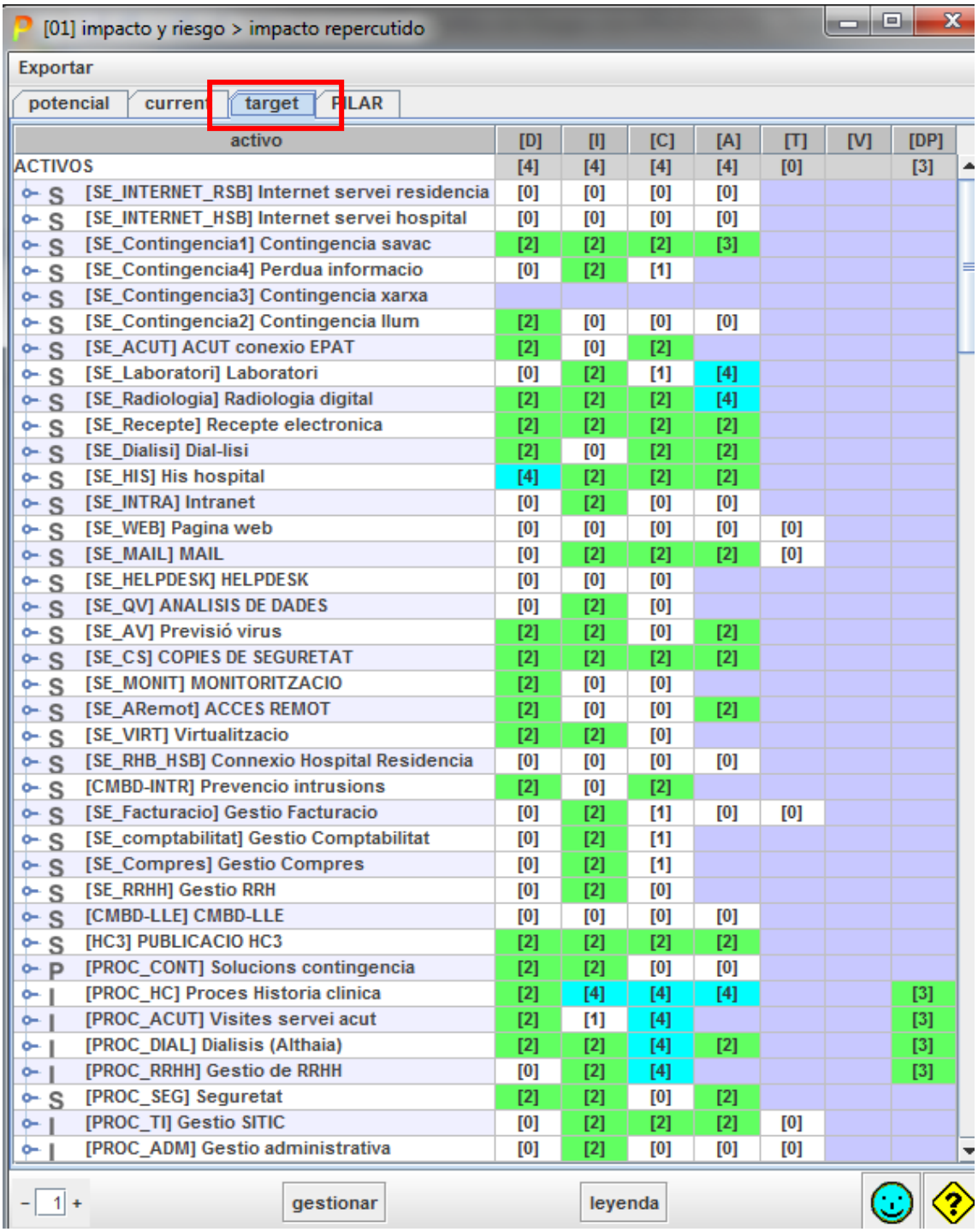
Ens mostra l'impacta repercutit , també: potencial , current , target i PILAR



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[9]	[9]	[9]	[7]	[3]
S [SE_INTERNET_RSB] Internet servei residencia	[1]	[0]	[2]	[2]	
S [SE_INTERNET_HSB] Internet servei hospital	[5]	[3]	[2]	[4]	
S [SE_Contingencia1] Contingencia savac	[7]	[7]	[7]	[6]	
S [SE_Contingencia4] Perdua informacio	[4]	[7]	[6]		
S [SE_Contingencia3] Contingencia xarxa					
S [SE_Contingencia2] Contingencia llum	[7]	[3]	[1]	[1]	
S [SE_ACUT] ACUT conexio EPAT	[7]	[4]	[7]		
S [SE_Laboratori] Laboratori	[5]	[7]	[6]	[7]	
S [SE_Radiologia] Radiologia digital	[7]	[7]	[7]	[7]	
S [SE_Recepte] Recepte electronica	[7]	[7]	[7]	[7]	
S [SE_Dialisi] Dial-lisi	[7]	[5]	[7]	[7]	
S [SE_HIS] His hospital	[9]	[7]	[7]	[7]	
S [SE_INTRA] Intranet	[4]	[7]	[4]	[4]	
S [SE_WEB] Pagina web	[1]	[3]	[1]	[4]	[1]
S [SE_MAIL] MAIL	[5]	[7]	[7]	[7]	[3]
S [SE_HELPDESK] HELPDESK	[4]	[5]	[2]		
S [SE_QV] ANALISIS DE DADES	[5]	[7]	[2]		
S [SE_AV] Previsió virus	[7]	[7]	[2]	[7]	
S [SE_CS] COPIES DE SEGURETAT	[7]	[7]	[7]	[7]	
S [SE_MONIT] MONITORITZACIO	[7]	[3]	[2]		
S [SE_ARemot] ACCES REMOT	[7]	[5]	[5]	[7]	
S [SE_VIRT] Virtualitzacio	[7]	[7]	[2]		
S [SE_RHB_HSB] Connexio Hospital Residencia	[3]	[1]	[2]	[3]	
S [CMBD-INTR] Prevencio intrusions	[7]	[4]	[7]		
S [SE_Facturacio] Gestio Facturacio	[5]	[7]	[6]	[3]	[3]
S [SE_comptabilitat] Gestio Comptabilitat	[5]	[7]	[6]		
S [SE_Compres] Gestio Compres	[5]	[7]	[6]		
S [SE_RRHH] Gestio RRH	[3]	[7]	[4]		
S [CMBD-LLE] CMBD-LLE	[5]	[5]	[3]	[3]	
S [HC3] PUBLICACIO HC3	[7]	[7]	[7]	[7]	
P [PROC_CONT] Solucions contingencia	[7]	[7]	[1]	[1]	
I [PROC_HC] Proces Historia clinica	[7]	[9]	[9]	[7]	
I [PROC_ACUT] Visites servei acut	[7]	[6]	[9]		
I [PROC_DIAL] Dialisis (Althaia)	[7]	[7]	[9]	[7]	
I [PROC_RRHH] Gestio de RRHH	[5]	[7]	[9]		
S [PROC_SEG] Seguretat	[7]	[7]	[3]	[7]	
I [PROC_TI] Gestio SITIC	[5]	[7]	[7]	[7]	[3]
I [PROC_ADM] Gestio administrativa	[3]	[7]	[5]	[5]	[3]



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[6]	[7]	[7]	[5]	[0]
S [SE_INTERNET_RSB] Internet servei residencia	[0]	[0]	[0]	[0]	
S [SE_INTERNET_HSB] Internet servei hospital	[3]	[0]	[0]	[1]	
S [SE_Contingencia1] Contingencia savac	[4]	[5]	[5]	[4]	
S [SE_Contingencia4] Perdua informacio	[1]	[5]	[4]		
S [SE_Contingencia3] Contingencia xarxa					
S [SE_Contingencia2] Contingencia llum	[4]	[0]	[0]	[0]	
S [SE_ACUT] ACUT conexio EPAT	[4]	[0]	[4]		
S [SE_Laboratori] Laboratori	[2]	[5]	[4]	[5]	
S [SE_Radiologia] Radiologia digital	[4]	[5]	[5]	[5]	
S [SE_Recepte] Recepte electronica	[4]	[5]	[5]	[4]	
S [SE_Dialisi] Dial-lisi	[4]	[2]	[4]	[4]	
S [SE_HIS] His hospital	[6]	[5]	[5]	[4]	
S [SE_INTRA] Intranet	[1]	[5]	[2]	[1]	
S [SE_WEB] Pagina web	[0]	[0]	[0]	[1]	[0]
S [SE_MAIL] MAIL	[2]	[3]	[3]	[4]	[0]
S [SE_HELPDESK] HELPDESK	[1]	[3]	[0]		
S [SE_QV] ANALISIS DE DADES	[2]	[5]	[0]		
S [SE_AV] Previsió virus	[4]	[5]	[0]	[4]	
S [SE_CS] COPIES DE SEGURETAT	[4]	[5]	[5]	[4]	
S [SE_MONIT] MONITORITZACIO	[4]	[1]	[0]		
S [SE_ARemot] ACCES REMOT	[5]	[2]	[2]	[4]	
S [SE_VIRT] Virtualitzacio	[4]	[5]	[0]		
S [SE_RHB_HSB] Connexio Hospital Residencia	[1]	[0]	[0]	[0]	
S [CMBD-INTR] Prevencio intrusions	[5]	[1]	[4]		
S [SE_Facturacio] Gestio Facturacio	[2]	[5]	[4]	[0]	[0]
S [SE_comptabilitat] Gestio Comptabilitat	[2]	[5]	[4]		
S [SE_Compres] Gestio Compres	[2]	[5]	[4]		
S [SE_RRHH] Gestio RRH	[0]	[5]	[2]		
S [CMBD-LLE] CMBD-LLE	[2]	[3]	[1]	[0]	
S [HC3] PUBLICACIO HC3	[4]	[5]	[5]	[4]	
P [PROC_CONT] Solucions contingencia	[4]	[5]	[0]	[0]	
I [PROC_HC] Proces Historia clinica	[4]	[7]	[7]	[5]	
I [PROC_ACUT] Visites servei acut	[4]	[2]	[6]		
I [PROC_DIAL] Dialisis (Althaia)	[4]	[4]	[6]	[4]	
I [PROC_RRHH] Gestio de RRHH	[2]	[5]	[7]		
S [PROC_SEG] Seguretat	[5]	[5]	[1]	[4]	
I [PROC_TI] Gestio SITIC	[3]	[5]	[5]	[4]	[0]
I [PROC_ADM] Gestio administrativa	[0]	[5]	[3]	[1]	[0]



A partir d'aquí obtenim tots els informes que conte un anàlisis fet segons mètode MAGERIT

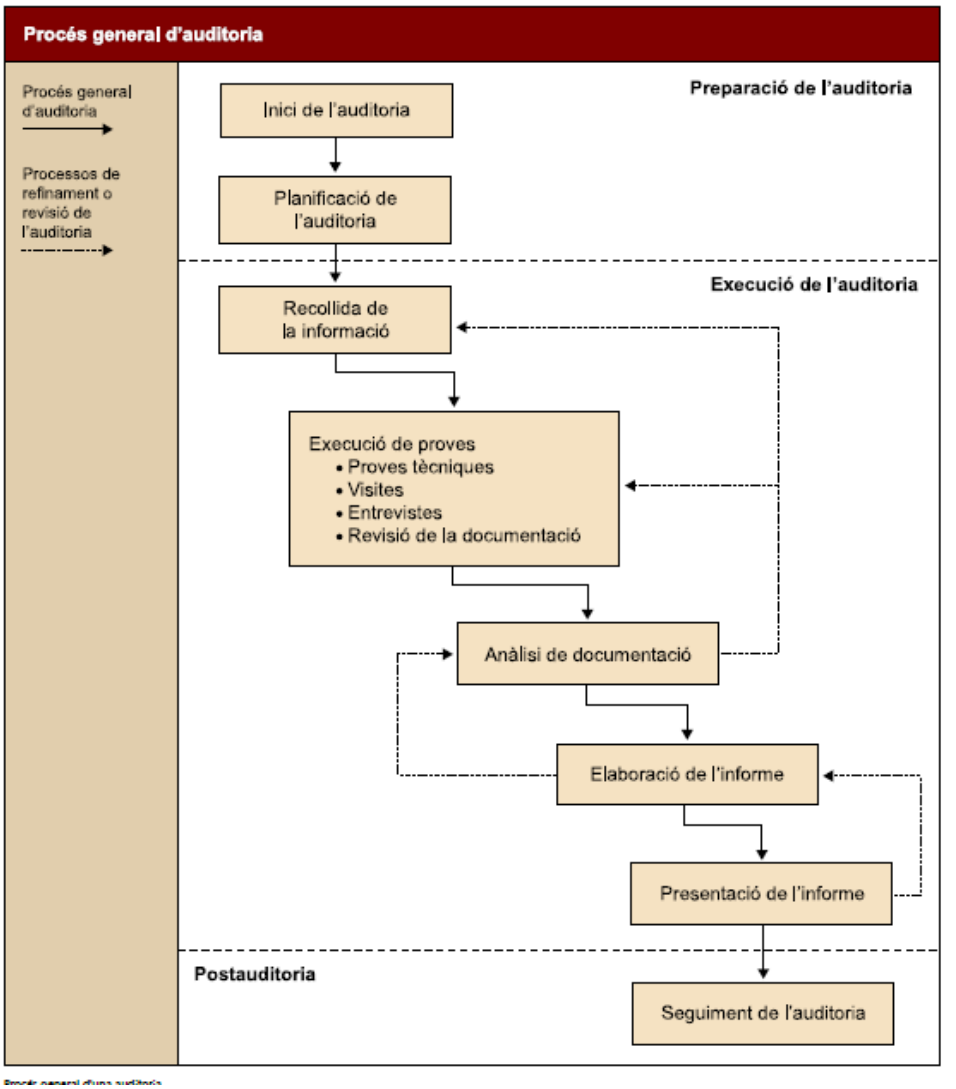
s'adjunta fitxer tfm que es pot obrir descarregant una versio gratuita de PILAR

2.4 QUARTA FASE: Auditoria ISO27001:2013

Anàlisis de compliment de l'organització davant la ISO: IEC 27001:2013, analitzant el control, maduresa i nivell de compliment

Al final s'ha de obtenir L'Informe de Auditoria.

El procés d'auditoria, és l'aplicació d'una revisió sistemàtica del compliment d'uns criteris d'auditoria que en aquest cas, son els de la ISO 27001, per tant descriuré aquests criteris i la manera com s'han avaluat per poder arribar a redactar l'Informe final.



2.4.1 Planificació de l'auditoria

En aquest cas ja tenim informació de la organització , tenim un marc legal, l'organigrama, les responsabilitats de cadascun en la organització de la seguretat i partim de un primer anàlisis de risc fet i un pla de projectes obtinguts d'aquest anàlisis i executats.

Amb tot això, primer decidirem quines dates i qui serà el responsable de l'execució de l'auditoria que en aquest cas serà interna amb personal de l'organització.

Quines proves farem i quina documentació demanarem ens vindrà indicat per la norma que volem auditar i les característiques pròpies de la organització auditada.

2.4.2 Com auditar la norma ISO 27001 : 2013

Aquesta norma internacional proporciona els requisits per establir , mantenir i millorar contínuament el sistema de gestió de la seguretat de la informació (SGSI).

Explicaré el que demana cada capítol i com s'ha organitzat l'auditoria segons aquest

Capítol 4 Context de l'organització

L'organització ha de determinar les parts interessades rellevants en el sistema de gestió de la seguretat de la informació i els requisits rellevants

Auditarem :

- document de l'Abast del SGSI ,
- organigrama,
- diagrama de processos de la organització

Capítol 5 Lideratge

La direcció ha d'estar alineada i demostrar lideratge respecte al SGSI

Auditarem :

- Recursos destinats al SGSI, segons Pla de projectes , tan de personal com de pressupost
- Factures,
- Entrevistes amb responsables de l'execució dels projectes
- Document de rols i funcions dintre de la seguretat
- Documents de Política de seguretat

Capítol 6 Planificació

S'ha d'identificar el risc, analitzar-lo, valorar la probabilitat de que es materialitzi aquest risc i segons el resultat, implementar controls i crear un plan per tractar aquest risc.

Auditarem :

- Com s'ha fet i si s'ha fet el anàlisis de risc, tota la documentació
- quina metodologia s'ha seguit,
- declaració d'aplicabilitat i exclusions
- quins controls s'han posat , documentació i registre dels mateixos
- qui es el responsable dels controls
- pla de projectes obtinguts de l'anàlisi del risc

Capítol 7 Suport

Hi ha d'haver els recursos necessaris per el SGSI, formar a les persones de l'organització, conscienciar-les, comunicar, documentar

Auditarem :

- s'ha fet formació al personal sobre seguretat?
- documentació existent sobre seguretat,
  - estàndards,
  - on es poden trobar
  - estan actualitzats
  - estan protocol·litzats (autor, data, versió, revisió, aprovació....)
  - com es comuniquen
  - qui els comunica

Capítol 8 Operació

S'ha de planificar i controlar els processos per complir el SGSI i tenir-ho documentat, auditar que es compleixi el pla de seguretat

Auditarem :

- Existeix una comissió de seguretat ?
- Demanarem les actes de les reunions
- Es fan auditories planificades ?
- Registres dels controls ex. sol·licituds accés

Capítol 9 Avaluació del desenvolupament

S'ha de avaluar l'eficàcia del SGSI , fen auditories que ha de revisar la direcció

Auditarem :

- Resultat de les auditories, documentació de les mateixes
- Sobretot les no conformitats i el seguiment d'aquestes
- Documents de conformitat per la direcció

Capítol 10 Millora

S'ha de reaccionar davant una no conformitat per millorar el sistema del SGSI

Auditarem :

- Accions realitzades davant les no conformitats

2.4.3 Personal implicat

Els requisits mínims per a un auditor intern ISO 27001 son experiència adequada i el coneixement demostrable en Seguretat de la Informació.

Ampli coneixement de la norma ISO 27001 i dels processos de seguretat de la informació.

Equip auditor

En aquest cas el nostre equip de auditoria esta format per:

- Cio de l'empresa amb amplis coneixements de ISO 27001
- Administrador de sistemes amb amplis coneixements de sgeuretat
- Secretaria tècnica amb responsabilitat sobre la documentació i els processos de negoci

Entrevistes

S'han dut a terme entrevistes amb

- Direcció de Recursos Humans
- tècnics de programació
- formació
- Directora d'infermeria
- Director mèdic
- Directora d'administració

Annexa 15 auditoria

4. Glossari

GLOSSARI DE TERMES.

Anàlisi de riscos

Utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos.

Dades de caràcter personal

qualsevol informació referent a persones físiques identificades o identificables. Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

Gestió d'incidents

Pla d'acció per atendre les incidències que es donin. A més de resoldre-ho d'incorporar mesures d'acompliment que permetin conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.

Gestió de riscos

Activitats coordinades per dirigir i controlar una organització pel que fa als riscos.

Incident de seguretat

Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del Sistema d'Informació.

Informació

És qualsevol conjunt de dades que tenen significat. L'Esquema Nacional de Seguretat es limita a valorar aquells tipus de informació que són rellevants per al procés administratiu i poden ser tractats en algun servei afecte a la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics. Per exemple, dades mèdiques, fiscals, administratius, contractacions, resolucions, notificacions, etc. En general, cal esperar que aquests tipus d'informació estiguin identificats en algun tipus d'ordenament general o particular de l'organisme, el que els confereix entitat pròpia i implica uns deures de l'administració respecte del tractament d'aquest tipus d'informació.

Política de seguretat

Conjunt de directrius plasmades en document escrit, que regeixen la forma en què una organització gestiona i protegeix la informació i els serveis que considera crítics.

Principis bàsics de seguretat

Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis.

Responsable de la informació

Persona o persones que tenen la potestat d'establir els requisits d'una informació en matèria de seguretat.

Responsable de la seguretat

El responsable de seguretat ha de determinar les decisions per satisfer els requisits de seguretat de la informació i dels serveis.

Responsable del servei

Persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.

Responsable del sistema

Persona que s'encarrega de l'explotació del sistema d'informació.

Servei

Funció o prestació exercida per alguna entitat oficial destinat a tenir cura interessos o satisfer necessitats dels ciutadans.

Sistema d'informació

Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, fer servir, compartir, distribuir, posar a disposició, presentar o transmetre.

Actius d'informació:

corresponen a elements que l'organització requereix per realitzar activitats de negoci o dur a terme qualsevol procés intern.

amenaces: són les situacions que desencadenen en un incident a l'empresa, realitzant un dany material o pèrdues immaterials dels seus actius d'informació.

vulnerabilitats: La vulnerabilitat d'un actiu de seguretat és la potencialitat o la possibilitat que es materialitzi una amenaça sobre l'actiu d'informació.

impactes: És el resultat o la conseqüència que es produeix quan una amenaça aprofita una vulnerabilitat per afectar un actiu d'informació.

GLOSSARI D'ABREVIATURES

ENS Esquema Nacional de Seguretat

FHSB Fundació Hospital Sant Bernabè

TIC Tecnologies de la Informació i les Comunicacions

ISO International Organization for Standardization

5. Bibliografia

CCN-STIC-402 Organització i Gestió per a la Seguretat dels Sistemes TIC. Desembre 2006.

CCN-STIC-801 ENS - Responsables i Funcions. 2010.

Llei 11/2007

Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics. BOE de 23 de juny del 2007.

Llei 15/1999

Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. BOE de 14 de desembre del 1999.

RD 1720/2007 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.

BOE de 19 de gener del 2008.

RD 3/2010 Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en el àmbit de la Administració Electrònica. BOE de 29 de gener del 2010.

Introducció a l'auditoria TIC i de seguretat TIC, Rafael Estevan de Quesada,PID_00239291)

https://ca.wikipedia.org/wiki/Hospital_Sant_Bernab%C3%A9 (23/02/2019)

http://www.hcsb.info/es (23/02/2019)

http://residenciasantbernabe.org/ (25/02/2019)

Memòries de la Fundació

https://www.idescat.cat/emex/?id=14&lang=es#h86007 (24/02/2019)

https://www.incibe.es (04/03/2019)

https://www.ccn.cni.es (08/03/2019)

https://cesicat.gencat.cat (21/03/2019)

6. ANNEXOS

1. Descripció detallada de la organització
2. Descripció dels sistemes d'informació
3. La Informació a la Fundació
4. Abast del pla director de Seguretat
5. Anàlisi de compliment inicial
6. Política de Seguretat
7. Procediment d'Auditories Internes
8. Gestió d'Indicadors
9. Procediment de Revisió per Direcció
10. Gestió de Rols i Responsabilitats
11. Metodologia de Anàlisis de Riscos
12. Declaració de Aplicabilitat
13. Pla de Projectes
14. Pla de projectes
15. Informe de Auditoria

Annexa 1 DESCRIPCIÓ DETALLADA DE LA ORGANITZACIÓ

L'Objectiu d'aquest document es descriure la Fundació Hospital Sant Bernabé

La Fundació

La Fundació Benèfica de l'Hospital de Sant Bernabé (d'ara en endavant FHSB), es va constituir a Berga l'any 1980, com una Fundació Pública de serveis, segons disposava l'article 85 e) del Reglament de Serveis de les Corporacions Locals.

El Ple de l'Ajuntament de Berga, en sessió de data 2 de juny de 1980 va aprovar definitivament els estatuts de l'Hospital de Sant Bernabé.

Els estatuts vigents a l'actualitat consten de 5 Títols i 29 articles, i van ser aprovats pel ple de l'Ajuntament de Berga, en sessió del 21 de gener de 1992 i publicats en el B.O.P. de Barcelona nº102 del 28 d'abril de 1992.

En el títol 1, article 1 dels estatuts trobem:

L'Hospital de Sant Bernabé de Berga, de remota existència, és una Fundació benèfica de naturalesa permanent, i té per objecte fonamental prestar assistència hospitalària als malalts pobres i o totes les altres persones que compleixin les condicions que reglamentàriament es determinin. Igualment, podrà gestionar una residencio d'avis.

D'acord amb l'actual Legislació de Règim Local, el Patronat té lo consideració d'organisme municipal autònom per l'acompliment de les finalitats de la Fundació.

Mentre que el títol 11, article 5 indica:

El govern, administració i representació de lo Fundació es confia, de manera exclusiva, al Patronat, nomenat amb subjecció al disposat en aquests Estatuts.

La Fundació Hospital Sant Bernabé és un organisme autònom depenent de l'Ajuntament de Berga que té com a objecte social l'atenció sanitària i social de la població de la Comarca del Berguedà.

L'Hospital Comarcal de Sant Bernabé és una organització sanitària comarcal que té com a finalitat prestar serveis de salut i atenció a la dependència a la població de la comarca del Berguedà. Té com a valors la professionalitat, el treball en equip, la

qualitat i el respecte a les persones. La seva missió és oferir als ciutadans i el seu entorn una atenció sanitària integral, de qualitat, amb continuïtat assistencial entre tots els nivells i centrada en les persones.

L'Hospital pertany a la Xarxa d'Hospitals d'Utilització Pública (XHUP), és una xarxa hospitalària de l'Institut Català de la Salut creada l'any 1985 per la Generalitat de Catalunya que inclou hospitals de propietat pública i de propietat privada per a donar assistència sanitària universal.

Orígens

Els orígens es remunten a l'edat mitjana.

l'orde dels hospitalers estava instal·lat des de principis de segle XIII a Berga on sembla que tenien una mena d'hospici o asil en el qual acollien viatgers i malalts, i a més, els donaven l'assistència que necessitaven.

Les primeres referències a Sant Bernabé apareixen uns quants anys més tard, entre finals de segle XIII i principis de segle XIV, quan els cònsols de la ciutat van comprar una casa a Berenguer de Prat, on els malalts pobres tenien acollida.

Al costat de l'edifici s'hi va construir una capella dedicada a sant Bernabé.

Segons Ramon Huch i Guixer, en el llibre Notes històriques de la ciutat de Berga l'hospital fou fundat gràcies a una donació feta per un mercader anomenat A. de Pinebret a mitjan segle XIV.

El primer llibre de cens conservat data dels anys compresos entre 1662 i 1722. A finals de segle XVII a causa de l'envelliment de l'edifici es va veure la necessitat de construir-ne un de nou, que fou inaugurat el 1726, el dia del seu patró, l'11 de juny. Posteriorment, ja a finals del segle XVIII i bona part del XIX, l'activitat de l'hospital fou més important, a causa de les contínues guerres amb França i les guerres carlines, la qual cosa va fer que es trobés sota una administració militar durant força temps.

Fou durant la primera guerra Carlina, més concretament el 1834, quan arribaren a l'hospital les germanes carmelites de Santa Joaquima de Vedruna.

A finals de 1980 es van aprovar uns nous estatuts segons els quals l'hospital havia d'estar regit per una junta presidida per l'alcalde i formada pel rector, i representants de l'Ajuntament, dels veïns de la ciutat i de l'equip directiu de l'hospital.

Futur

La Generalitat gestionarà directament a través d'una nova empresa pública que crearà, l'hospital comarcal Sant Bernabé de Berga .

Salut Catalunya central és el nom de l'empresa que s'ha de crear per gestionar el centre berguedà i tindrà representació del territori. Ara s'inicia un procés per concretar tot aquest canvi. Probablement també es crearà un òrgan de tipus consultiu amb una àmplia representació de la comarca.

La gestió es farà a través d'una nova empresa que crearà el CAT Salut per dur a terme aquesta tasca específicament. El consistori farà una cessió d'ús de les instal·lacions sanitàries que són de la seva propietat. D'aquesta manera es resoldrà una vella assignatura pendent sobre el model de governança del centre .

"Volem donar-li una governança més sòlida perquè sabem que això permetrà fer una millor gestió". Acompanyat de l'alcaldessa Montse Venturós, el conseller Comín va explicar que amb aquesta mesura "estem garantint la viabilitat i el futur" de l'hospital Sant Bernabé.

El fet de que L'hospital que és de titularitat municipal el gestioni directament un ajuntament, genera problemes al consistori. De fet en el passat mandat es va fer l'intent de canviar la forma jurídica del centre, una operació que va generar debat social i la creació d'una plataforma en defensa de la sanitat pública al Berguedà. Finalment , aquesta operació no va reeixir per les limitacions a la creació de nous organismes que imposa la llei de racionalitat de l'administració local (RSAL) als ajuntaments endeutats com el berguedà.

Des d'aleshores aquest tema estava pendent de resolució. El conseller Antoni Comín va fer unes declaracions on explicava que la Generalitat assumiria directament la gestió del centre sanitari berguedà .

Marc geogràfic

El Berguedà

Actualment la Fundació consta de 2 edificis l'Hospital y Residencia i un edifici annexa que s'ha fet a l'Hospital fa poc temps situats a Berga, comarca del Berguedà.

Hospital Sant Bernabé

IL·LUSTRACIÓ 6 HOSPITAL SANT BERNABÉ

42° 06′ 23″ N, 1° 51′ 07″ E

adreça :Carretera de Ribes s/n 08600-berga

Residencia Sant Bernabé

IL·LUSTRACIÓ 7 RESIDENCIA SANT BERNABÉ

adreça :Carretera de Solsona s/n 08600-berga

Població	Berguedà	Catalunya
Densitat de població. 2018		
Superfície (km2)	1.185,25	32.108,00
Densitat (hab./Km2)	33	236,7
Població. Por sexe. 2018		
Hombres	19.502	3.730.326
Dones	19.602	3.869.739
Total	39.104	7.600.065
Poblacions. Por grups de edat. 2018		
De 0 a 14 anys	5.113	1.177.134
De 15 a 64 anys	24.412	5.001.510
De 65 a 84 anys	7.507	1.185.318
De 85 anys y mes	2.072	236.103
Total	39.104	7.600.065
Naixements. Por sexe. 2017		
Nens	133	34.462
Nenes	133	32.341
Total	266	66.803
Defuncions. Por sexe. 2017		
Hombres	264	33.075
Dones	279	33.090
Total	543	66.165
Creixement de la població. Taxa bruta por 1.000 habitants. 2017		
Taxa bruta de natalitat	6,83	8,88
Taxa bruta de mortalitat	13,94	8,8
Creixement natural	-7,11	0,08
Creixement migratori	8,5	6,29
Creixement total	1,39	6,32

Governança

Òrgans de govern

El govern, administració i representació de lo Fundació es confia, de manera exclusiva, al Patronat

L'actual Junta de Patronat, consta dels següents membres:

Com a presidenta, l'alcaldessa de Berga

El Gerent de la Fundació
El President del Consell Comarcal del Berguedà
Un representant del Consell Comarcal del Berguedà
Cinc vocals en representació de l'Ajuntament
Dos persones a proposta de l'equip de Govern de l'Ajuntament de Berga

El secretari de l'ajuntament

Òrgans de gestió

Sr. Enric Ballabriga i Garcia, gerent

Sra. Anna Franch i Parella, directora econòmic- financera

Sra. Joana Rodríguez i Codina, directora d'Infermeria

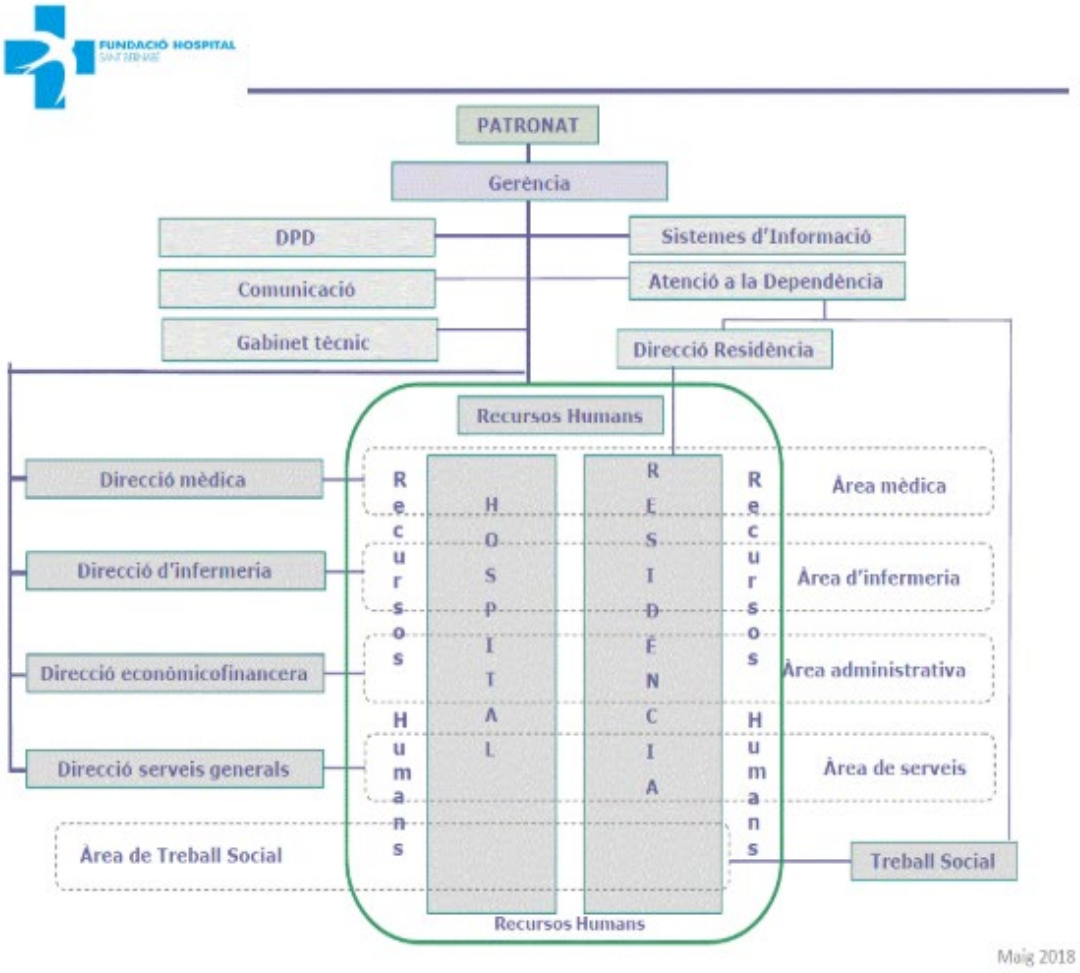
Sra. Mariona Morera i Sala, directora de Recursos Humans

Sra. Ester Cardona i Prat, directora assistencial de la Residència

Sra. Betlem Vilaró i Pasquets, responsable de la Unitat d'Atenció al Client

Sra. Anna Rodríguez i Codina, secretària tècnica

Organigrama

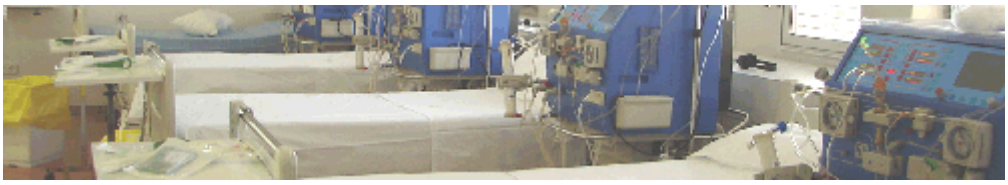


IL·LUSTRACIÓ 8 ORGANIGRAMA

Serveis que ofereix la Fundació

Hospital

Serveis ambulatoris



Cirurgia i especialitats

- Cirurgia general i digestiva
- Otorinolaringologia
- Oftalmologia
- Urologia
- Cirurgia vascular
- Cirurgia plàstica
- Cirurgia ortopèdica i traumatologia
- Rehabilitació

Clínica del dolor
Consulta preanestèsica
Ginecologia i obstetrícia
Medicina física i rehabilitació
Medicina interna i especialitats

- Cardiologia
- Digestiu
- Endocrinologia
- Hematologia
- Nefrologia i hemodiàlisi
- Neurologia
- Oncologia mèdica
- Pneumologia
- Reumatologia
- Unitat de Diagnòstic Ràpid (UDR)

Pediatria i neonatologia
Cirurgia ambulatòria

- Cirurgia major ambulatòria (CMA)
- Cirurgia menor ambulatòria (Cma)

Gabinets de diagnòstic per la imatge

- Ecografia convencional
- Ecografia Doppler
- Mamografia
- RX convencional
- RX amb contrast
- RX intervencionista

Hospital de dia

- Hospital de dia d'endocrinologia
- Hospital de dia mèdic
- Hospital de dia oncològic
- Hospital de dia psicogeriàtric

Laboratori d'anàlisis clíniques

- Bioquímica
- Hematologia
- Microbiologia

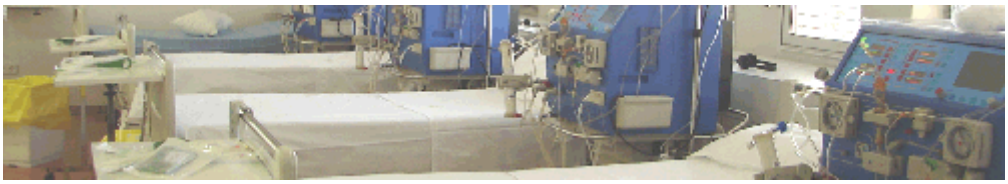
Proves complementàries

- Audiometria
- Ecografia
- Electrocardiografia
- Electromiografia
- Espirometria
- Fibrobroncoscòpia
- Fibrocolonoscòpia
- Fibroendoscòpia digestiva alta
- Laringoscòpia
- Otoendoscòpia
- Polisomnografia
- Prova d'esforç
- Punció esternal
- Rectoscòpia
- Ressonància
- Test d'alè

TAC

- Crani
- Columna
- Cara i coll
- Tòrax, abdomen, pelvis
- Sistema musculoesquelètic
- Diagnòstic a distància (nits, caps de setmana i festius)

Serveis hospitalaris



Cirurgia i especialitats
Cirurgia general i digestiva
Cirurgia plàstica
Oftalmologia
Otorinolaringologia
Urologia
Cirurgia ortopèdica i traumatologia
Ginecologia i obstetrícia
Hospitalització a domicili
Medicina interna i especialitats
Cardiologia
Digestologia
Endocrinologia
Hematologia
Nefrologia i hemodiàlisi
Neurologia
Oncologia mèdica
Pneumologia
Reumatologia
Pediatria

Serveis sociosanitaris

EAIA - Equip d'Atenció Integral Ambulatòria

ESI - Equip de Suport Integral

Hospital de Dia Psicogeriàtric

UFISS - Unitat Funcional Interdisciplinària Sociosanitària

ULLE - Unitat de Llarga Estada

UMEP - Unitat de Mitjana Estada Polivalent

La Fundació Hospital Sant Bernabé disposa de diferents serveis sociosanitaris amb una gran polivalència, que atenen persones amb malalties cròniques físiques o psíquiques, amb pluripatologia, malaltia invalidant o malaltia terminal de manera integral, amb un equip multidisciplinari que vetlla per la prevenció, la planificació i la coordinació assistencial de manera que els recursos siguin equitatius.

Residencia

Els serveis que ofereix són:

Residència assistida

Servei d'acolliment residencial amb caràcter permanent o temporal per a persones grans dependents, que no tenen un grau d'autonomia suficient per desenvolupar les activitats de la vida diària i necessiten constant atenció i supervisió, i que per les circumstàncies sociofamiliars requereixen la substitució de la llar.

Acolliment diürn

El centre de dia és un servei diürn i d'assistència a les activitats de la vida diària per a persones grans amb dependència.

Programa Descans

En conveni de col·laboració amb l'Ajuntament de Berga, disposen d'un programa de suport a les famílies que tenen a càrrec seu una persona gran amb dependència, i els ofereix un espai de descans i alleujament.

El programa consisteix a facilitar l'ingrés de la persona gran a la residència de forma temporal. La durada d'aquestes estades pot ser d'un mes a l'any en períodes sencers o partits, segons les necessitats de la família.

Gent Gran a Casa

Amb l'objectiu de facilitar que la gent gran amb dependència pugui continuar vivint en el seu entorn i, alhora, donar suport als cuidadors.

Serveis d'atenció domiciliària

En conveni amb els serveis socials dels ajuntaments de Berga, Gironella, Gósol, Saldes i Vallcebre, així com amb el Consell Comarcal, proporcionen serveis d'atenció domiciliària.

Aquest servei s'adreça a la persona gran amb problemes de dependència per a les activitats bàsiques de la vida diària (AVD) i per a les activitats instrumentals de la vida diària (AVDI). Es concreta en neteges, àpats a domicili, atencions personals, cobertura de les absències dels treballadors familiars (cadascun en el nivell que necessiti).

Berguedà Ajudes Tècniques

Conjuntament amb el Consell Comarcal, gestionen el projecte Berguedà Ajudes Tècniques.

En el marc del servei Gent gran a casa i amb l'objectiu de millorar l'atenció i la qualitat de vida de les persones amb manca d'autonomia i de les seves famílies.

Aquest inclou:

Un servei de valoració, orientació i informació als usuaris i les seves famílies i la instrucció en el funcionament dels ajuts per mitjà d'una Terapeuta Ocupacional.

Cessió del material adequat (grues, llits articulats elèctrics, matalassos antiescares, seient de banyera, cadira de dutxa…, així com el manteniment i les reparacions.

La Fundació en xifres

Recursos Humans

Personal assistencial facultatiu	43,86
Personal assistencial no facultatiu	195,19
Personal no assistencial	55,70
Total	294,75

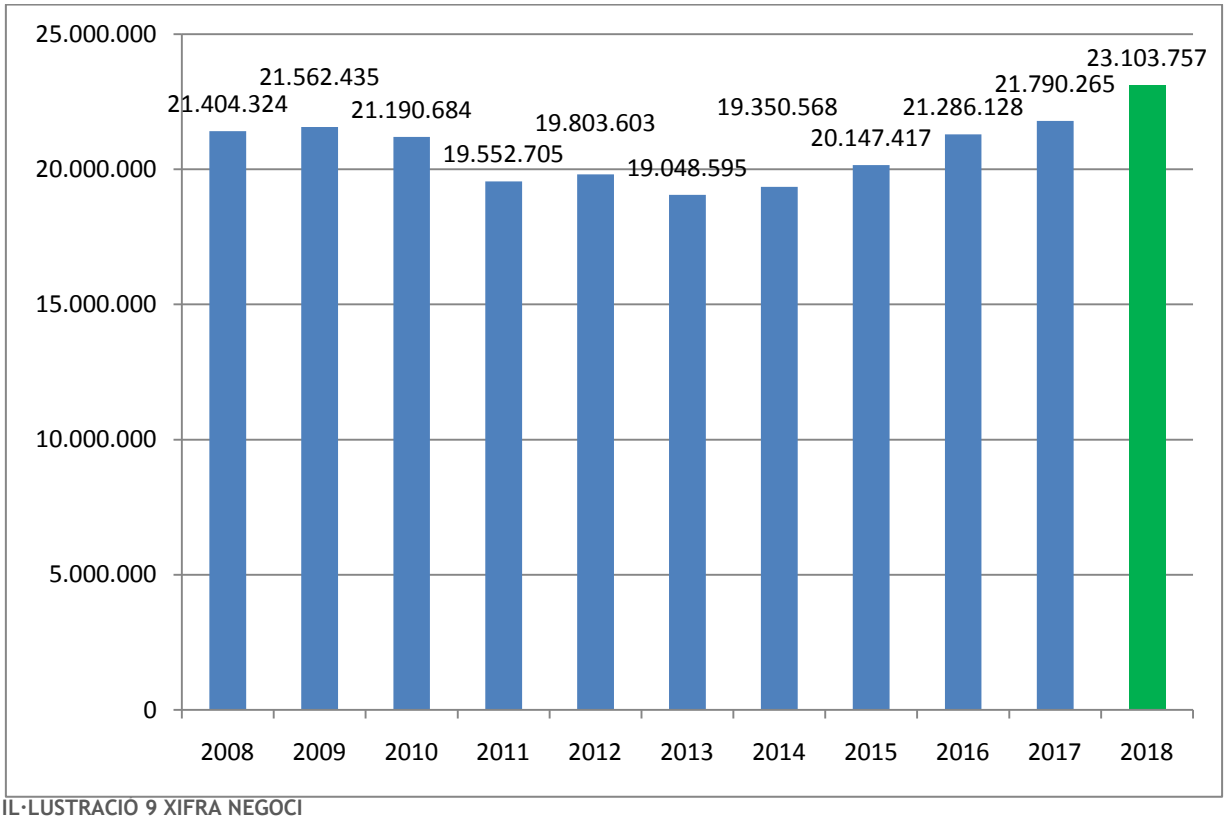
Recursos estructurals

Llits de l'Hospital	100
Llits d'hospitalització d'aguts	57
Llits sociosanitaris	
Convalescència	15
Llarga estada	23

Llits de la Residència	64
Consultes externes	17
Quiròfans	3
Quiròfan de cirurgia menor	1

Recursos econòmics

Xifra de negoci euros/any



IL·LUSTRACIÓ 9 XIFRA NEGOCI

Marc normatiu

Normativa de caràcter comunitari

•Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la i protecció de les persones físiques paper que fa a l'Tractament de dades personals ia la lliure Circulació d'aquestes dades i paper qual és deroga la Directiva 95/46 / CE (Reglament general amb protecció de dades)

Llei estatal

• Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text refós de la llei de propietat intel·lectual.

• Llei 59/2003, de 19 de desembre, de signatura electrònica.

• Llei 56/2007 o Llei per a l'Impuls de la Societat de la Informació.

• Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics

• Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals

• Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.

Llei autonòmica

• Llei 26/2010 del 3 d'agost de règim jurídic i Procediment de les Administracions Públiques de Catalunya

• Llei 16/2015 de 21 de juliol de simplificació de l'activitat administrativa de l'Administració de la Generalitat i dels Governs Locals de Catalunya il 'impuls de l'activitat econòmica.

• Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

Reglaments

• 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.

• Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.

• Reial Decret 704/2011, de 20 de maig, pel qual s'aprova el Reglament de protecció de les infraestructures crítiques.

• Reial Decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

• Reial Decret 3/2010, de 8 de gener (BOE de 29 de gener), pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.

• Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.

• Reial Decret 704/2011, de 20 de maig, pel qual s'aprova el Reglament de protecció de les infraestructures crítiques.

https://ca.wikipedia.org/wiki/Hospital_Sant_Bernab%C3%A9

http://www.hcsb.info/es

http://residenciasantbernabe.org/

Memòries de la Fundació

https://www.idescat.cat/emex/?id=14&lang=es#h86007

Annexa 2 Sistemes d'informació de la Fundació

L'Objectiu d'aquets document es descriure els Sistemes d'informació de la Fundació Hospital Sant Bernabé

Departament de Sistemes d'informació, tecnologia de la informació i comunicacions de la Fundació Hospital Sant Bernabé

Aquest departament gestiona i dona suport als sistemes d'informació a les tecnologies de la informació i a la comunicació tan a l'Hospital Sant Bernabé com a la Residencia Sant Bernabé.

Missió del departament

Proposar i gestionar eficient i eficaçment, els recursos, la infraestructura,els serveis tecnològics i la informació institucional mitjançant l'administració, manteniment i desenvolupament dels sistemes d'informació i serveis informàtics que donin suport als processos desenvolupats pels usuaris interns i externs amb consonància amb el Pla estratègic de la fundació

Ubicació física

Físicament es troba ubicat a la cinquena planta del edifici Hospital Sant Bernabé , despatxos 514 i 516 a la carretera de Ribes s/n Berga (086000)

Horaris

El departament esta obert des de les 8 del mati fins les 7 de la tarda, els dies laborables

Els dies festius i vigílies hi ha una persona del departament de guàrdia localitzable a les següents hores

Divendres i vigílies de festius intersetmanals de les 20h fins les 24h

Dissabte, diumenge i festius intersetmanals de les 8h fins les 24h

Personal que l'integra

Responsable del departament (Coordinació i projectes) :

Montserrat Magnet Sabata

Estudiant Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Enginyeria Tècnica d'Informàtica de Sistemes

Graduat en Multimèdia

Expert en Drupal i seguretat

Adjunt al responsable del departament (anàlisis de dades)

Lluis Venturós Pedrosa

Enginyer informàtic

Postgrau Administració GNU/Linux

Màster Intel·ligència de Negoci i Big Data

Responsable de sistemes i comunicacions

David Butxaca

Enginyer informàtic

Màster en Gestió de les Tecnologies de la Informació

Expert en Nutanix

Responsable de desenvolupament

Albert Fontquerni

Certificats MCD i MCE en Microstrategy, Microstrategy, tardor 2015.

Màster en Tecnologies de la Informació (MTI), Universitat Politècnica de Catalunya, juny 2011.

Enginyer Tècnic en Informàtica de Gestió, Universitat Politècnica de Barcelona(UPC), juny 2009 (Projecte Final de Carrera: Signatura digital de documents machine-readable).

Tenim també segons els mesos un estudiant de practiques de FP de l'escola Xarxa de Berga.

Valors

Personal altament qualificat i especialitzat

Treball en equip, motivació, implicació

Compromís

Responsabilitat

Integritat

Capacitat de resposta davant les dificultats

Coneixement de la Fundació tan del personal com dels processos

Equip integrat en la població

Punts febles

L'equip ha de gestionar els mateixos processos (compres, facturació, Historia clínica, Radiologia, farmàcia, enviament de CMBD ...) en un Hospital de les nostres característiques que en un Hospital gran, però amb molt menys personal i menys pressupost.

Funcions

Desenvolupament de sistemes:

Analitzar dissenyar i desenvolupar els sistemes informàtics i supervisar els que son de responsabilitat de empreses externes per recolzar la execució i gestió de processos interns, amb alta disponibilitat seguretat i con fiabilitat .

Establi controls i procediments de seguretat per salvaguardar els recursos informàtics de la Fundació i complir la llei RGPD

Administrar recursos informàtics:

Administrar i assegurar la disponibilitat de la xarxes comunicacions servidors i estacions de treball

Suport a usuaris:

Prevenir mantenir i corregir hardware software i la connectivitat institucional de les estacions de treball dels usuaris per poder treballar de manera optima amb els productes institucionals

Assessorar i oferir coneixement a la direcció per que es puguin prendre les millors decisions

Detectar les necessitats operatives i de formació dels usuaris

Tots els integrants del departament menys el personal de practiques, estem adscrits al servei de guàrdies localitzables.

Tots donem suport durant els nostra horari de treball a les incidències de hardware o software dels usuaris, (menys les impressores, totes les incidències/reparacions de maquinari les resolem des del mateix departament).

INFRAESTRUCTURA TECNOLÒGICA

Fins l'any 2018 hi havia un sol CPD a l'hospital que constava d'un clúster de 3 servidors de virtualització amb VMware i un servidor on hi havia instal·lat el Virtual Center.

En El servidor de vitalització hi corrien 51 servidors (Windows i GNU/Linux).

També hi havia un clúster de 2 servidors físics d'Oracle i un servidor pel programa de laboratori.

El sistema de backup estava format per un servidor de backup amb Veeam Backup i un appliance Symantec Backup Exec 3600.

Una cabina MSA 1500 que ténia doble controladora actiu-passiu, amb 1 safata de discs SCSI MSA-30 (6 discs 72Gb 15k i 8 discs 300Gb 10k) i 1 safata de discs SATA MSA-20 (14 discs de 1Tb 7,2k). Els Backups i rèpliques de les VM s'emmagatzemen en aquesta cabina.

El sistema d'emmagatzemament estava implementat en un metroclúster NetApp, format per dues cabines NetApp FAS3140 i una cabina d'emmagatzemament de backup.

Antic rack de servidors

Cabina NetApp

L'any 2018 la fundació modernitza la infraestructura tecnologia de l'hospital i es proveeix d'una infraestructura molt mes evolucionada tecnològicament

Formada per Dos centres de dades amb una arquitectura hiperconvergent d'alt rendiment.

12 | DIMARTS, 21 D'AGOST DEL 2018

SOCIETAT ▸ BERGUEDÀ

L'hospital de Berga actualitza els seus sistemes centrals informàtics de dades

▶El centre disposarà d'una infraestructura d'alt rendiment amb més espai, més segura i més moderna

D.C. BERGA

■ L'Hospital Comarcal Sant Bernabé de Berga actualitzarà els seus sistemes centrals de dades, que és «on es genera i es tracta totes les dades i informació de l'hospital» el Centre de Processament de Dades (CPD), segons ha explicat a **Regió7** Montse Magnet, responsable de Sistemes d'Informació del centre sanitari. Aquesta acció s'emmarca dins del projecte «d'actualització dels sistemes d'informació, on hi ha el canvi de servidors i cabina d'emmagatzemen de fitxers del Centre de Processament de Dades (CPD)» que es paga amb una subvenció de la Diputació. Costa 100.000 euros i s'ha adjudicat a l'empresa Sercom Informativa SL.

Actualment, el centre sanitari berguedà té una infraestructura tradicional «basada en un clúster de servidors, cabina de discos de fibra òptica i una sèrie de sistemes per gestionar els serveis que, amb

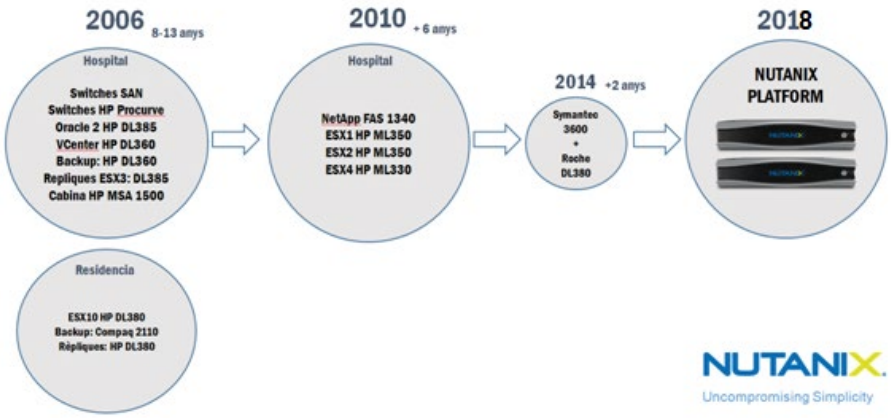
ARXIU PARTICULAR

Montse Magnet, Albert Fontquerni, Lluís Venturós i David Butxaca, l'equip informàtic de l'hospital davant de l'actual Centre de Processament de Dades (CDP), que conté els servidors antics

apostar pel nou sistema anome- gència que afectés el CPD princi-

IL·LUSTRACIÓ 10 NOTICIA REGIO7

Evolució de les solucions

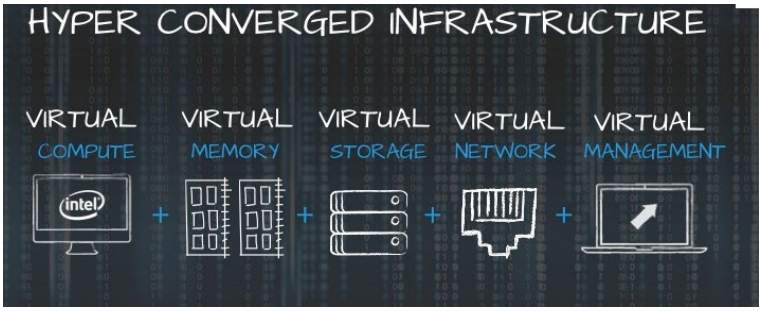


IL·LUSTRACIÓ 11 EVOLUCIÓ SOLUCIONS

*ESTALVI ENERGÈTIC MOLT IMPORTANT, ENTRE UN 50 % I UN 70%

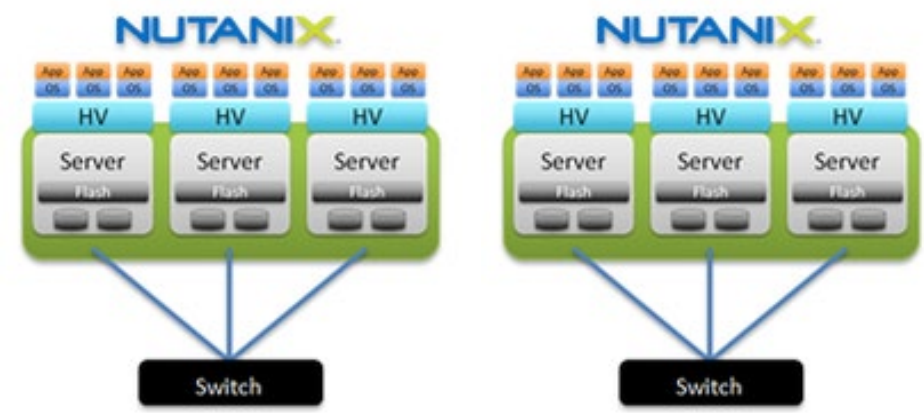
NUTANIX

Característiques generals de la solució INSTAL.LADA



Es una Plataforma Hiperconvergent de 6 nodes, host físics, 3+3, que combinen computació i emmagatzemament amb tecnologia SSD i HDD en un mateix equipament

Combinem aquesta solució amb 4 switches de HP Aruba, que permeten una connectivitat altament fiable a uns costos molt efectius



1. la computació i emmagatzematge resideixen en la mateixa Plataforma basada en tecnologia "Web-Scale"

2. La solució es recolzar-se exclusivament en una xarxa Ethernet amb possibilitat de connectivitat a 10 Gbps.

3. El sistema proporciona un mínim de tres controladors d'emmagatzematge per dotar de redundància i evitar situacions tipus Split-Brain.

4. La plataforma de virtualització es totalment redundant, en cas de fallada dels components de maquinari, el sistema es capaç de reconstruir ràpidament les dades que falten i aquest procés no generarà degradació del Sistema.

5. La solució esta protegida contra fallada simultània de dos elements de maquinari del mateix tipus, sense pèrdua de dades (controlador, discos i/o servidor).

6. Els recursos: la potència de càlcul, les dades, l'eina de gestió i les metadades son distribuïts.

7. La solució es el més compacta possible, estalviant espai en el Datacenter, consum energètic i cooling.

ESCALABILITAT

8. La solució permet un increment lineal dels recursos de l'entorn afegint nous servidors. S'entén per recursos la capacitat d'emmagatzematge, capacitat de procés i memòria.

9. La solució te possibilitat de barrejar servidors de diferents capacitats (CPU, RAM, Emmagatzematge) per poder ajustar-se a les necessitats de l'entorn o noves càrregues de treball.

10. Possibilitat d'afegir servidors d'emmagatzematge a la Infraestructura de forma transparent, no suposaria un increment de costos de llicenciament al programari de virtualització.

11. L'escalabilitat de la solució pot ser gestionada per una única consola. El creixement de l'entorn no genera més complexitat en la gestió.

EMMAGATZEMAMENT

12. La solució inclou "tiering" automàtic en lectures i escriptures de Dades entre els diferents tipus de discos 'ràpids' SSD / Flaix (hot data) i discos 'lents' (cold data).

13. La solució inclou mecanismes d'optimització d'espai en discos Sòlids. (Deduplicació SSD)

14. La solució incloure mecanismes d'optimització d'espai en Discos rotacionals. (Compressió i Deduplicació) i te la possibilitat de configurar la funcionalitat de compressió podent seleccionar in-line o post-process.

15. Protecció de Dades: El sistema inclou mecanismes de protecció de Dades seguint aquests requeriments bàsics:

a. Un mínim d'una còpia de dades permetent la pèrdua d'un servidor amb tot l'emmagatzematge corresponent.

b. Possibilitat d'ampliar la resiliència de dades amb dues còpies de dades permetent casos extrems com la caiguda de dos servidors de forma simultània amb l'emmagatzematge corresponent.

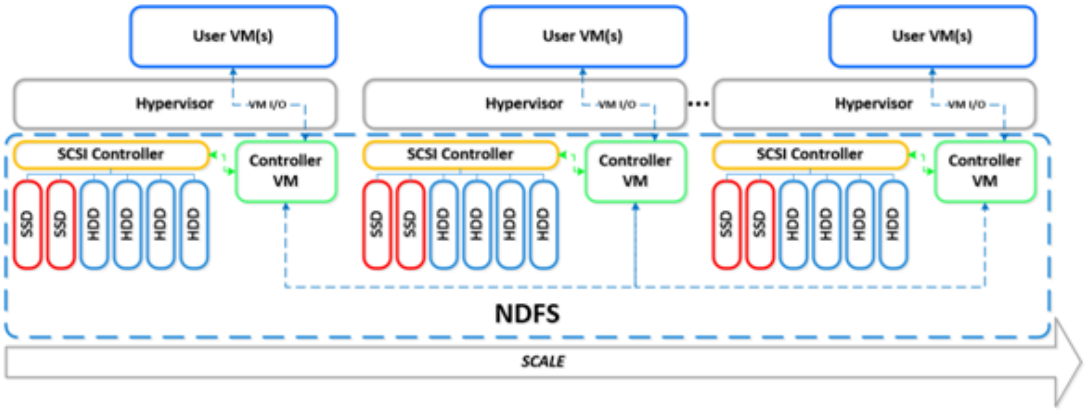
c. Repartició de Dades entre xassís de capacitats similars quan el nombre de xassís és superior a tres. Aquest mecanisme permet resiliència de dades amb la caiguda de quatre servidors de forma simultània.

d. La pèrdua de diversos discos o servidors de forma no simultaniejada es suportada assegurant-se la disponibilitat de la dada i continuïtat del servei.

IL·LUSTRACIÓ 12 INSTAL•LANT NUTANIX CPD1

Característiques de cada node

(CLUSTER 1, DE 3 NODES – CPD 1 / CLUSTER 2, DE 3 NODES – CPD 2)



IL·LUSTRACIÓ 13 CLÚSTER NUTANIX

Per cada clúster:

1 Nutanix NX-1365-G5 amb 3 NODES

Característiques x node:

2 x Xeon 2.10GHz 8 cores Broadwell E5 2620v4 20M Cache

8 x 16GB DDR4 Memory Module (128GB por nodo)

2 x 6TB 3.5" HDD

1 x 480GB 3.5" SSD

1 x 1GbE Dual SFP+ Network Adapter

Recursos totals:

6 processadors

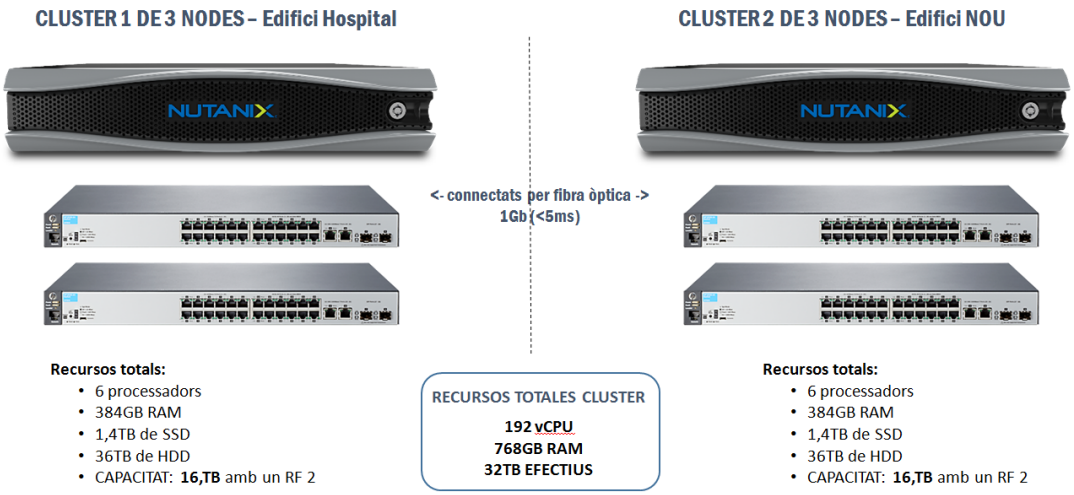
384GB RAM

1,4TB de SSD

36TB de HDD

3 X 1GbE

CAPACITAT EFECTIVA: 16,TB amb un RF 2 (redundant factor)



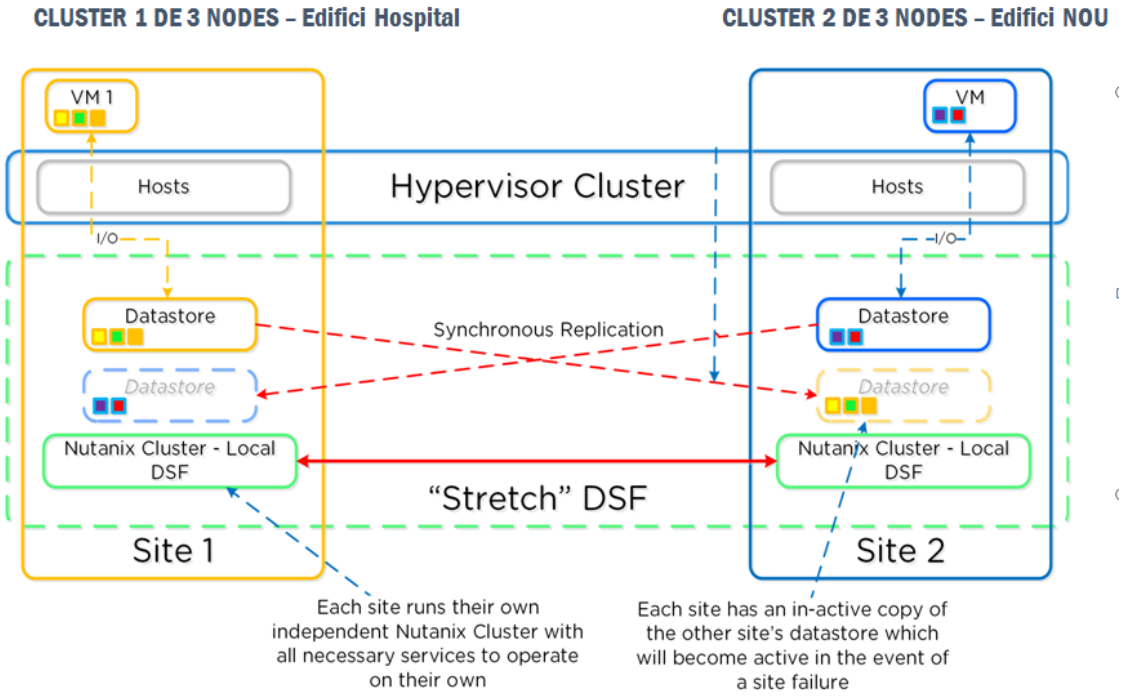
IL·LUSTRACIÓ 14 2 CLÚSTERS REDUNDANTS

Cada clúster fa de Backup Remot i DR de l'altre, podent activar les VM de les que es fan backups/rèpliques quan cau el que les estava executant

La replicació pot ser síncrona o asíncrona entre 2 Nutanix

Quan la replicació es síncrona el RPO es zero i el RTO també

Quan la replicació es asíncrona el RPO màxim es de 1h i el RTO s'apropa a zero



IL·LUSTRACIÓ 15 REPLICACIÓ SÍNCRONA

Connectivitat

4 SWITCHES de core HP Aruba 2530-24G per disposar de doble camí (HA)

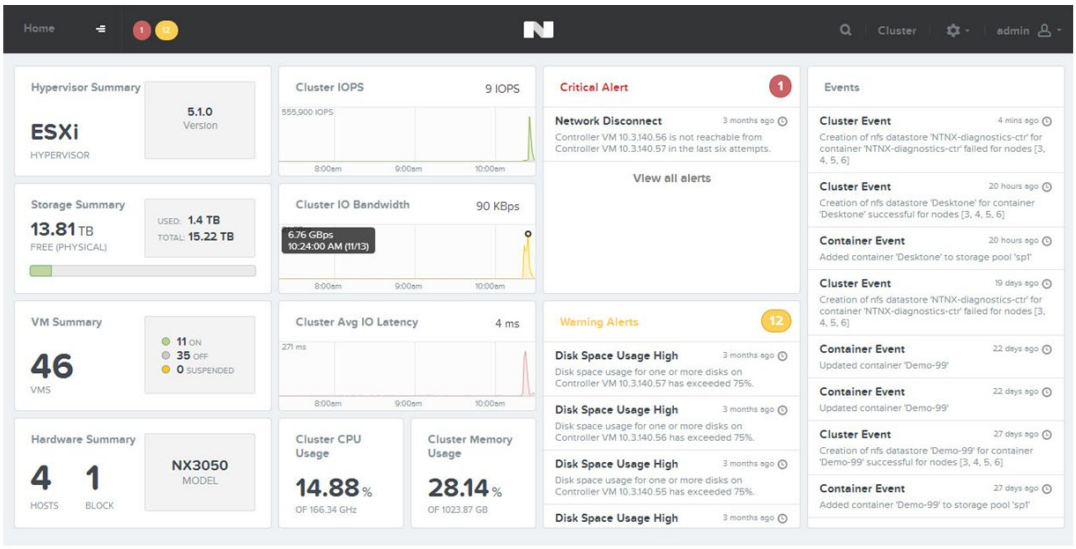
2 switches a l'edifici de l'Hospital

2 switches a l'edifici nou

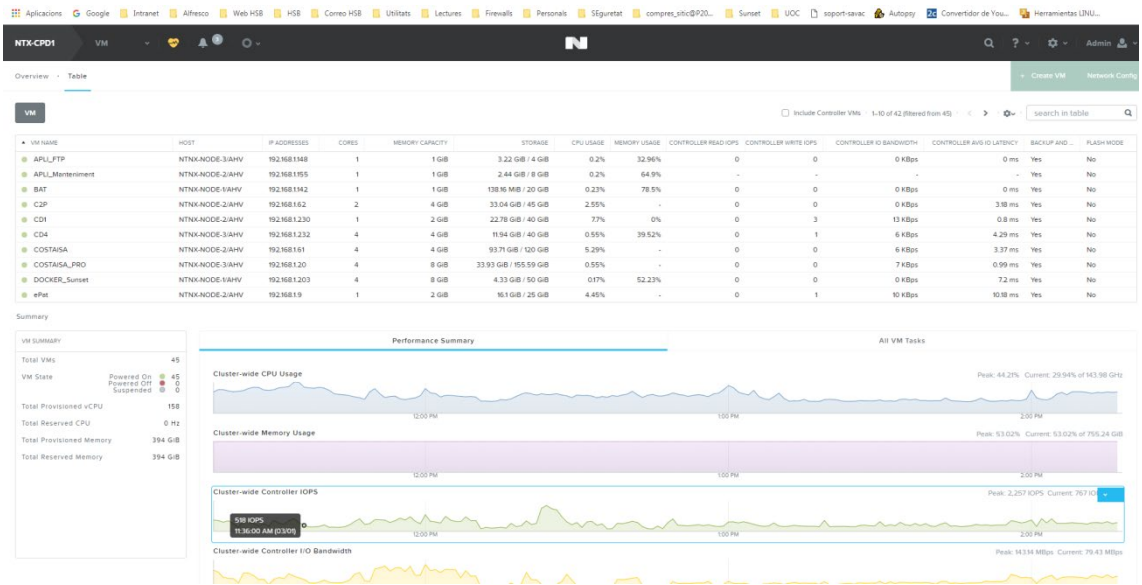
- ACLs
- Seguretat d'accés
- Prioritització de trànsit
- sFlow

- IPv4 / IPv6
- Enllaços SFP + 10GbE
- IMC
- Connexions a 1GbE entre Switches de Core i Nutanix

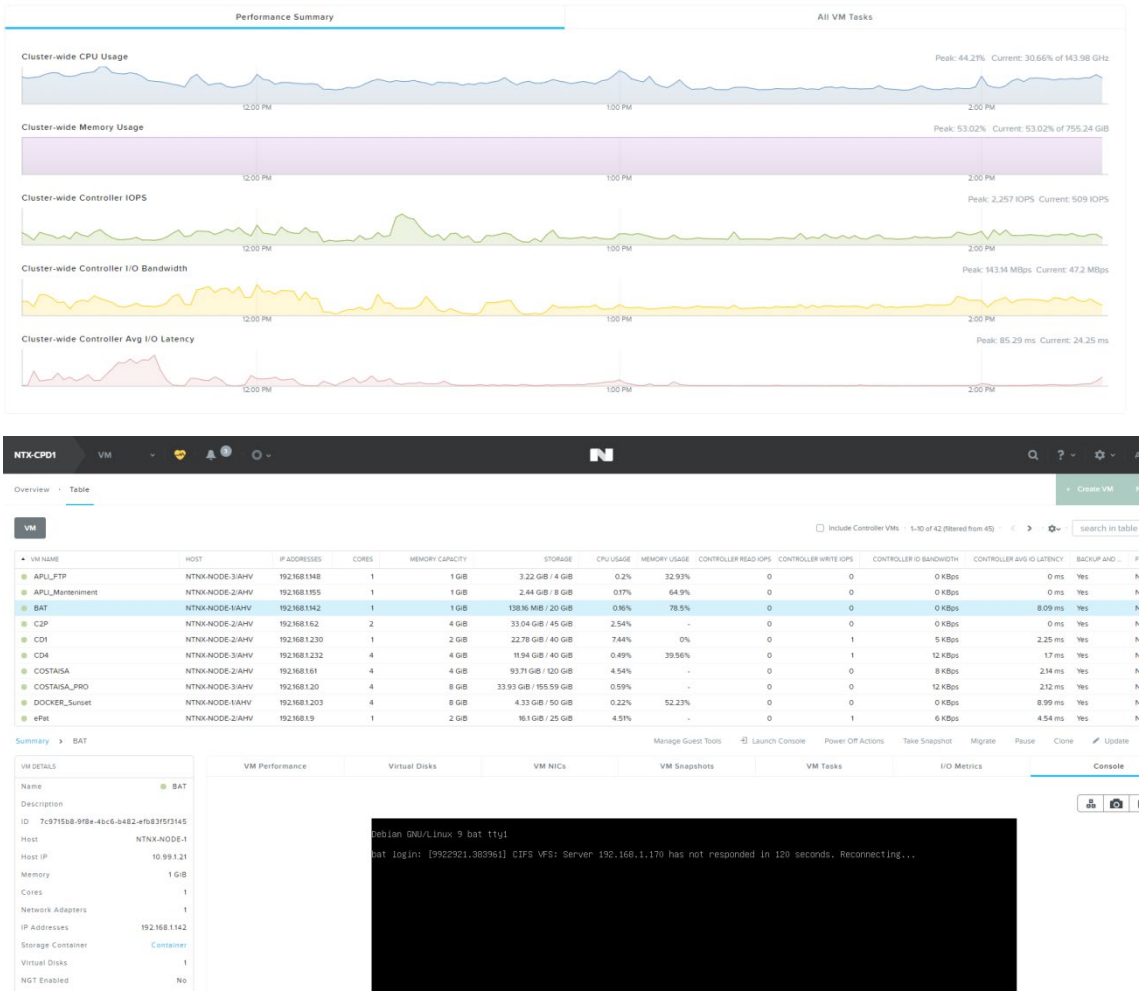
Consola de administració de nutanix



IL·LUSTRACIÓ 16 CONSOLA NUTANIX



Taula de VM



IL·LUSTRACIÓ 17 CONSOLA VM

Consola de una Vm, en concret anomenada BAT

ARQUITECTURA FÍSICA DEL SISTEMA

En aquest moment la infraestructura tecnològica de la Fundació està formada per:

CPD's, Servidors físics i virtuals,cabines de emmagatzematge , elements de xarxa, impressores, ordinadors clients, telèfons mòbils, aparells de electromedicina, routers, firewalls.

Centres de processament de dades

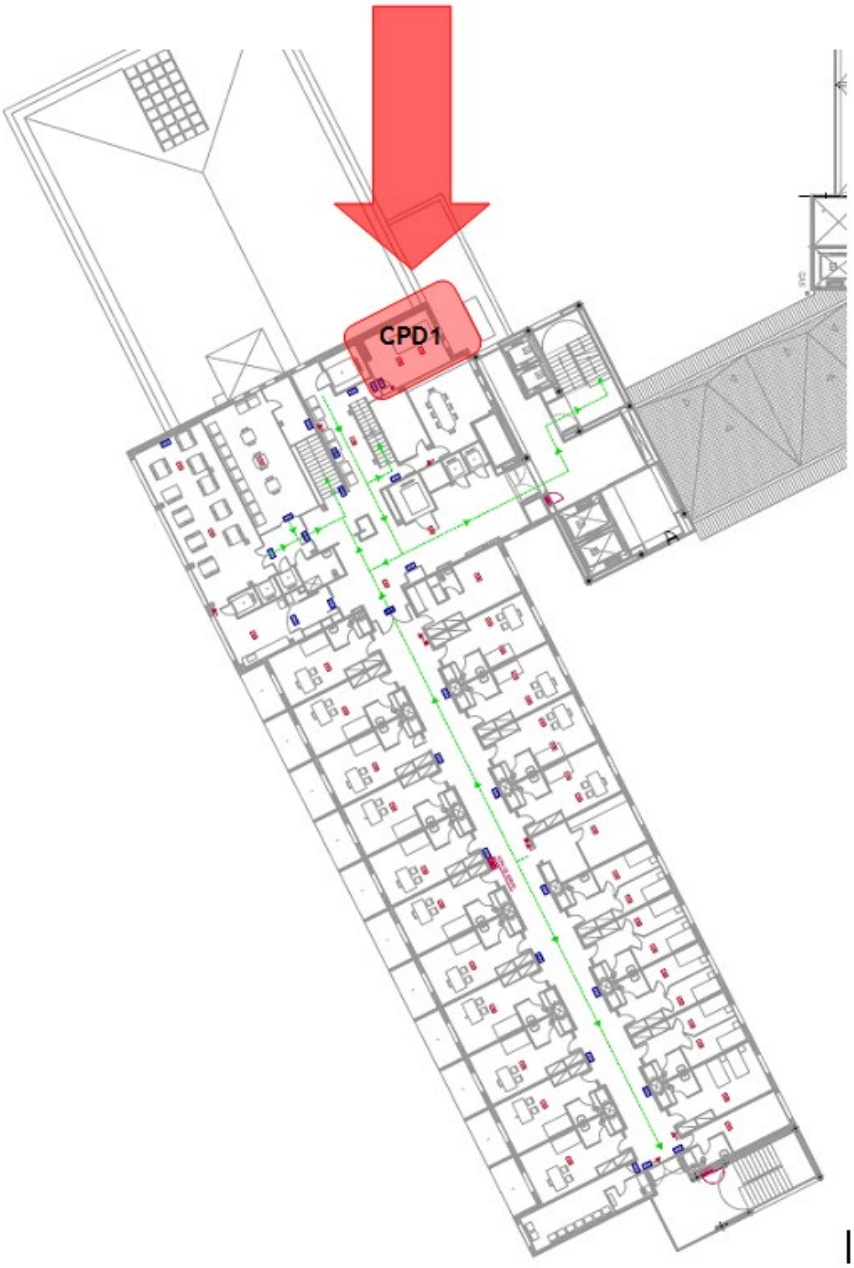
- CPD 1 Hospital
- CPD 2 Hospital
- CPD 3 Residencia

Un centre principal de processament de dades (en endavant CPD1) on trobem els servidors, les cabines d'emmagatzematge de dades, els tallafocs, la connexió al nus sanitari, els switchs de fibra del Nus sanitari, de enllaç a la Residencia, enllaç a Internet un ADSL, 2 firewallsles i altres infraestructures bàsiques per al funcionament de la part informàtica de la fundació, Cabines d'emmagatzematge NetApp

Un segon CPD (en endavant CPD2) al edifici nou de l'hospital que consisteix en un armari INUIT IT POWER & COOLING que allotja un node dels nous servidors hiperconvergents i una cabina de copies synology.

Un tercer CPD a la Residencia , molt mes petit , nomes consta d'un armari rack, amb 2 servidors , 1 firewall, 1 ADSL .

CPD1 principal situat a la pl. 5 de l'hospital,



IL·LUSTRACIÓ 18 PLÀNOL CPD1

Entrada a CPd1

IL·LUSTRACIÓ 19 ENTRADA CPD1

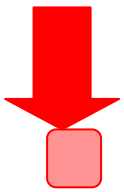
 Protecció antiincendis  càmera

 aires acondicionats

situats a CPD1 tenim actualment 2 firewalls de nova generació WATCHGUARD FIREBOX M400 que configuren un clúster actiu – passiu, comprats l'any 2017

IL·LUSTRACIÓ 20 FIREWALLS

CPD 2 – Hospital



IL·LUSTRACIÓ 21 PLÀNOL CPD2

localització PL0 Hospital, edifici nou

S'ha escollit per allotjar el CPD2 una solució d'armari compacte degut a que el impacte econòmic d'aquest producte és molt menor que una solució convencional.

Consta de 2 zones: una freda, que és la part anterior on estaran ubicats tots els servidors, aparells d'aire condicionat, SAI, Rack monitoring system i quadre de magnetos i a la part posterior, que seria el calent, es troba el retorn de l'aire calent, les connexions dels equips en el quadre de magneto i les PDUs per a l'alimentació dels servidors.

L'estructura es de doble xapa,a l'interior conte llana de roca, material que afavoreix l'aïllament tèrmic i ens ofereix resistència al foc. Protecció contra incendis 30 min.

Sistema de control de monitorització de sensors temperatura / humitat, fum, obertura. Connectivitat via IP amb la unitat central. Diagnòstic visual Llum LED de 3 colors

Porta unitat de refrigeració i SAI intern.

Control d'accés per teclat numèric.

IL·LUSTRACIÓ 22 REFRIGERACIÓ ARMARI INUIT

IL·LUSTRACIÓ 24 ARMARI CPD2

Armari CPD2

IL·LUSTRACIÓ 23 INTERIOR CPD2

Interior : Nutanix + Synology Cpd2

CABINA COPIES a CPD2

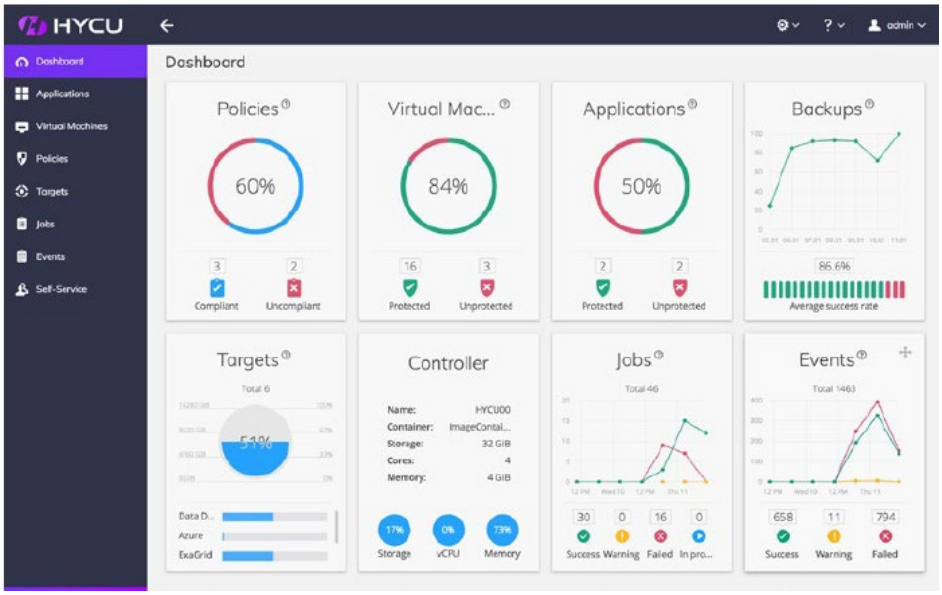
NAS SYNOLOGY RS3617XS+ 12BAYS

DISCO SATA WD RED PRO 6TB 5 discos

Per que hem escollit Hycu com a software de copies ?

- HYCU és la primera solució de còpia de seguretat desenvolupada exclusivament per Nutanix, integrada amb el hipervisor de Nutanix, Acropolis HV.
- Utilitza les API de Nutanix per fer la còpia de seguretat i les restauracions.

- No té costos addicionals de llicències de Windows, BBDD, etc.
- Es la única solució que fa còpia de seguretat de l'AFS de Nutanix (sistema de fitxers).
- Es desplega en molt poc temps.
- Basada en polítiques no en tasques, que no s'han de programar.
- Consola orientada a que l'administració sigui molt senzilla el que augmenta la
- productivitat
- Fa còpies de seguretat consistents a nivell d'aplicació.
- Fa una còpia de seguretat de SQL, Oracle, Exchange.



IL·LUSTRACIÓ 25 COPIES SEGURETAT /HYCU

CPD 3 Residencia

Ubicació Pl-1 edifici Residencia

IL·LUSTRACIÓ 26 INTERIOR CPD3

servidors Físics:

ESX

1 ESx ,amb WMWARE allotja:

VM : Residencia, CD3 (replica controladors de domini) , Backup

El Backup fa repliques de les MV cap a l'hospital i cap al segon servidor Repliques

Repliques

Armari Rack CPD3

Firewall

hi ha un model WATCHGUARD T30

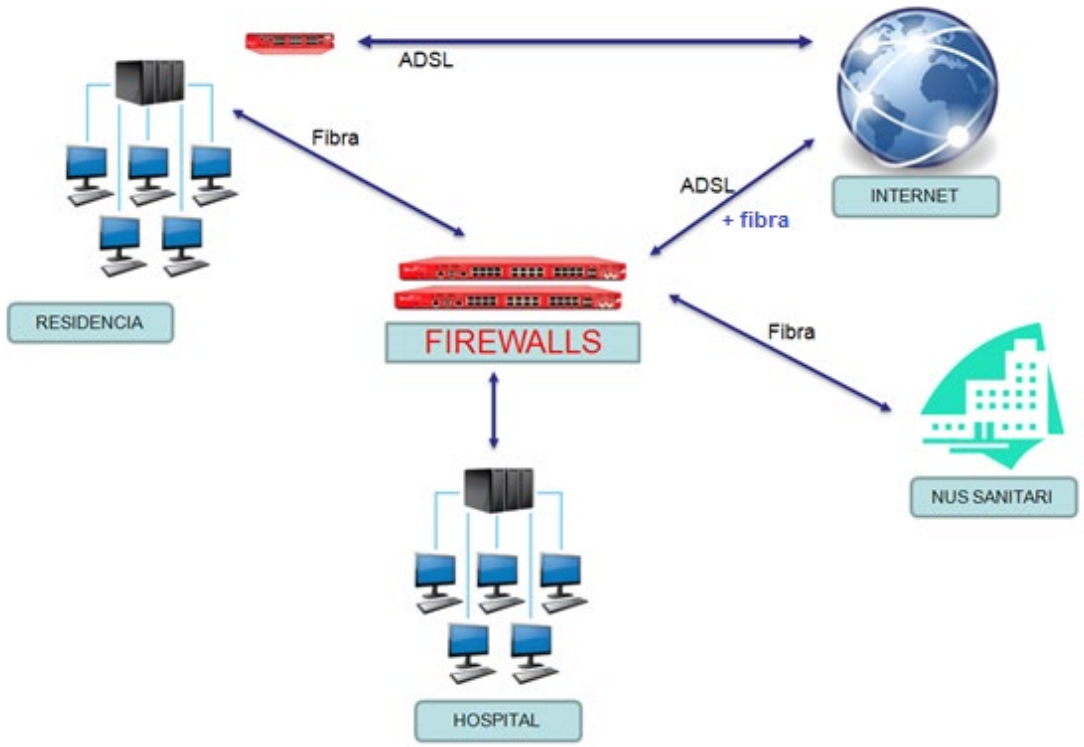
Armari rack Residencia

Xarxes

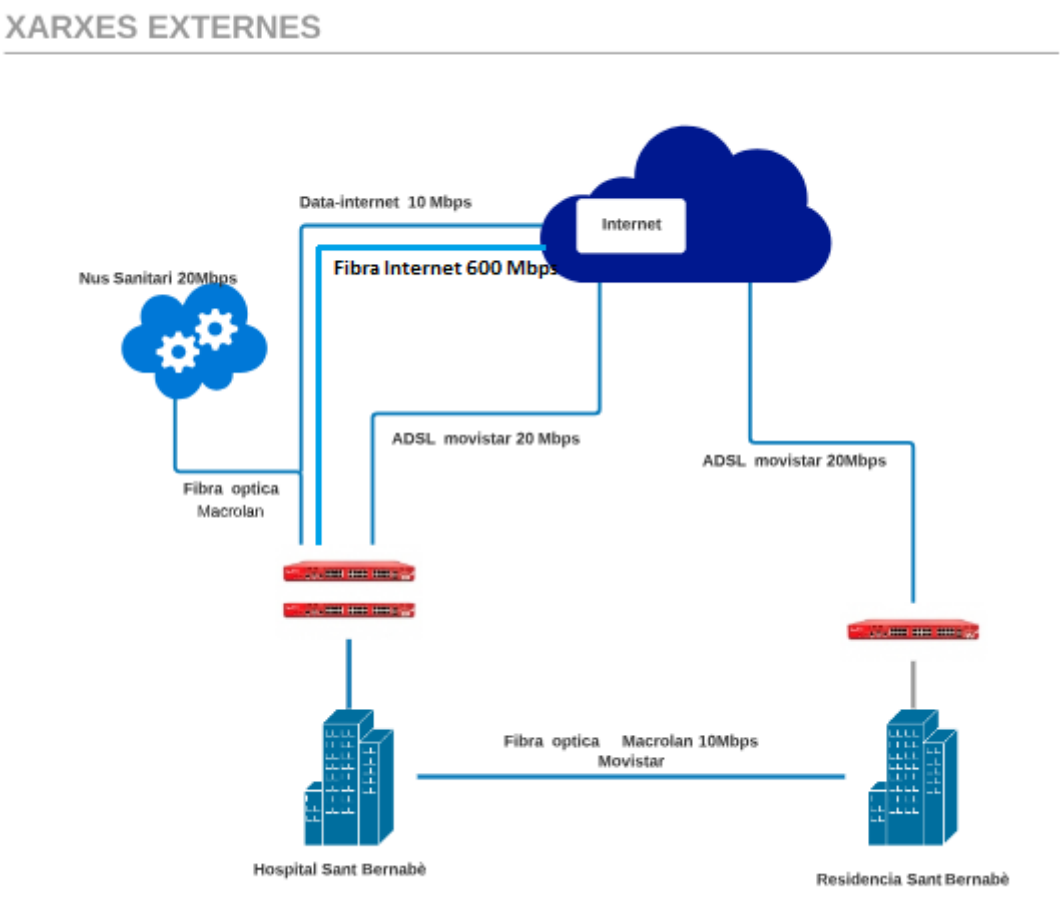
L'hospital i la Residencia estan connectats entre si amb fibra metrocluster, tan l'un com l'altre estan connectats a Internet protegits amb un firewall , en el cas de l'Hospital aquest es redundant.

També en el cas de l'Hospital, la connexió a Internet es doble, amb un ADSL i una fibra de 600Mbps simètrics, i l'hospital disposa a mes d'una altra fibra extra que li dona connexió al anomenat Nus sanitari amb 20 Mbps (xarxa privada de connexió entre Hospitals de Catalunya per compartir informació Sanitaria)i datainternet amb 10 Mbps.

IL·LUSTRACIÓ 27 XARXES



IL·LUSTRACIÓ 28 XARXES EXTERNES



L'Hospital te 7 armaris de distribució de xarxa connectats entre si i cap als 2 CPD's amb fibra

L'electrònica de xarxa d'aquests armaris racs s'ha de modernitzar dons ja te 7 anys.

En el cas de l'edifici vell de l'Hospital hi han 3 armaris ,

Planta 0, que distribueix cap als punts de Planta -1, Planta 0 , Planta 1

Planta 3 dona xarxa a la planta 3 i 4

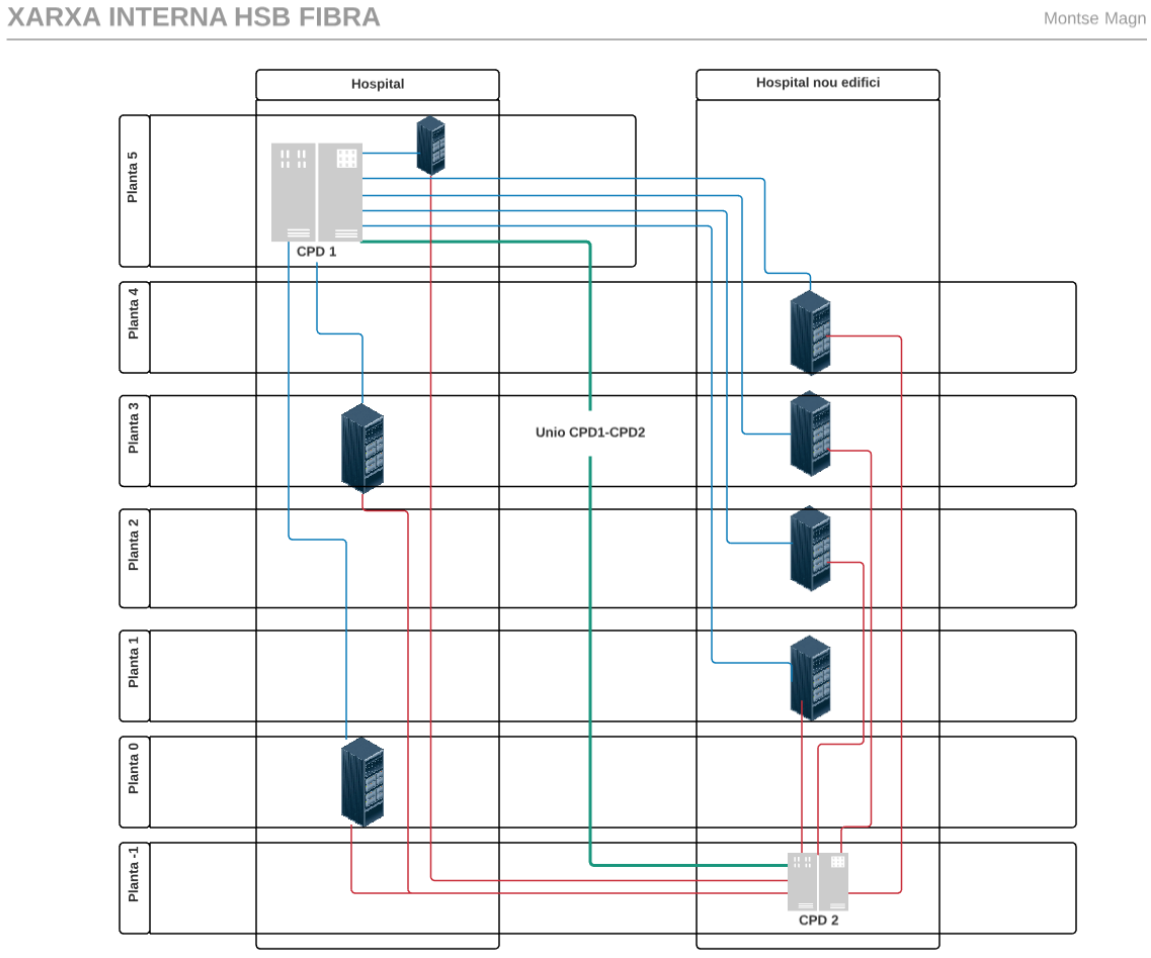
Planta 5 distribueix la xarxa a la planta 5

En l'edifici nou hi ha un armari per planta menys planta 0 que s'alimenta amb el de planta 1.

La connexió cap als punts finals es a traves de coure categoria 5.

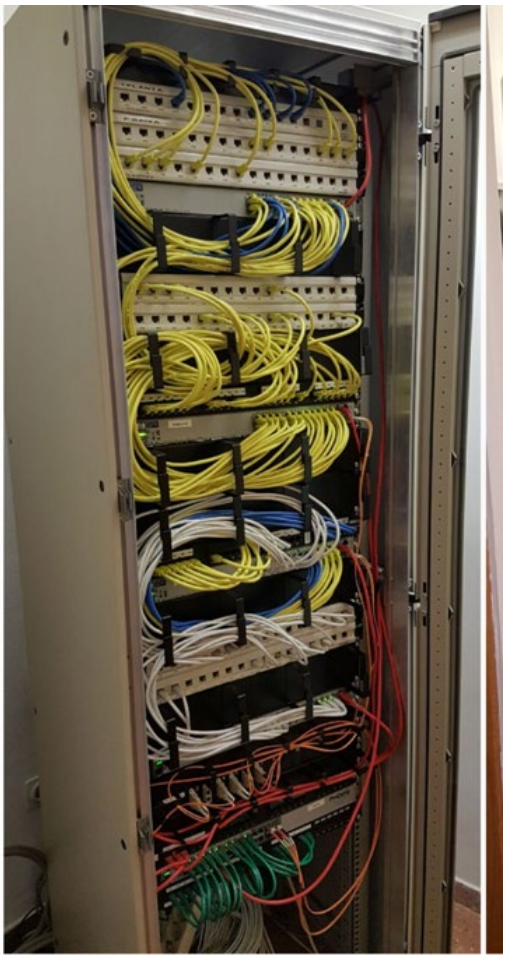
Cablejat Xarxa interna hospital

IL·LUSTRACIÓ 29 XARXA HOSPITAL



Els 2 CPDs del hospital i els armaris rack estan connectats entre si amb fibra

IL·LUSTRACIÓ 30 RACK PLANTA 0



armari rack Planta 0

Llistat Switchs

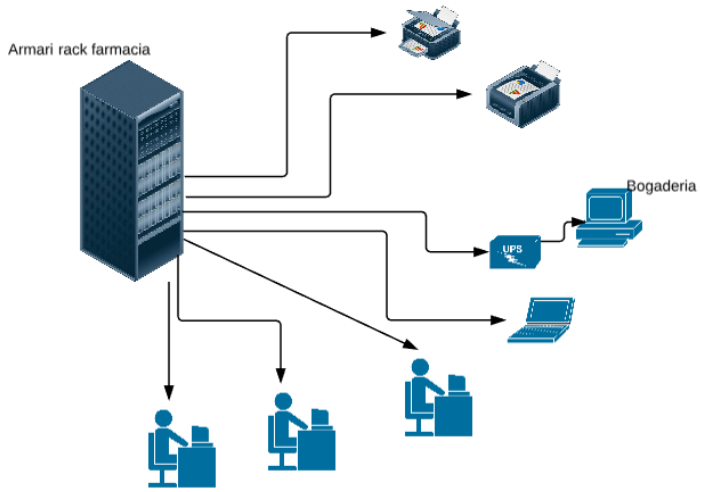
Hospital edifici vell i residencia

Rack		Switch	Model
Planta baixa	1	SW046	HP OfficeConnect 1820 24G PoE+ J9983A
Planta baixa	2	SW042	HP OfficeConnect 1820 24G PoE+ J9983A
Planta baixa	3	SW041	HP Procurve 2626 J4900A
Planta baixa	4	SW044	HP Procurve 2610-24-PWR J9087A
Planta baixa	5	SW045	HP Procurve 2510G-24 J9279A
Planta baixa	6		Cisco SF 300-48
Planta 3a	1	SW3	HP OfficeConnect 1820 24G PoE+ J9983A
Planta 3a	2	SW029	HP OfficeConnect 1820 24G PoE+ J9983A
Planta 3a	3	SW043	HP Procurve 2610-48-PWR J9089A
Planta 5a	1	SW05	HP OfficeConnect 1820 24G PoE+ J9983A
Planta 5a	2	SW04	HP Procurve 2626 J4900A
CPD1	1	SW031	HP Procurve 5308XL
CPD1	1	SW032	HP Procurve 5308XL
CPD1	1		Huawei CE6810-24S2Q-LI
CPD1	1		Huawei CE6810-24S2Q-LI
CPD2	1		Huawei CE6810-24S2Q-LI
CPD2	1		Huawei CE6810-24S2Q-LI

EN. Planta 1a	1	SW1.1	3Com 4210
EN. Planta 1a	2	SW1.2	3Com 4210 (Aturat)
EN. Planta 2a	3	SW2.1	3Com 4210 (Aturat)
EN. Planta 3a	4	SW3.1	3Com 4210
Residencia	1	SW046	HP Procurve 2626 J4900A

Xarxa Residencia LAN

IL·LUSTRACIÓ 31 XARXA RESIDENCIA



Un únic armari situat al CPD 3 dona servei a 14 punts amb ordinadors clients i 4 punts amb impressores en xarxa.

No disposen de wifi.

EQUIPS CLIENTS

Disposem de 211 equips clients, es troben als diferents despatxos mèdics, consultoris i àrees de treball

D'aquests els del control d'infermeria per administrar la medicació son portàtils.

Els de dintre els quiròfans i algun altre també.

Els pc clients de l'àrea de reanimació a Quirofan son all-in-one per aconseguir una area amb menys pols.

La majoria son marca Hp o dell amb processador Intel-core i3 o i5, amb 4 GB RAM mínim i un monitor, el 90% > 19" .

El sistema operatiu es Windows 7 Professional , 64bits o 32 segons.

Els programes instal·lats a cada client predeterminats son:

- Bitdefender endpoint security tools
- Netsupport notyfi
- Pdfcreator
- Office 2003 o 2007
- Savac
- VNC
- Ocsinventory
- Java
- TunneUp utilitis
- Bit4id
- Safesing

IL·LUSTRACIÓ 32 EQUIPS QUIRÒFAN

PC clients area reanimació Quiròfans

IMPRESSORES

L'hospital te contractat un servei de impressió de pagament per copia amb l'empresa ControlGroup, es fan càrrec del subministrament als dos centres l'Hospital i la Residencia

Serveis:

Subministrament i gestió de la reposició de consumibles (el paper d'impressió es proporcionat per FHSB). La gestió del reaprovisionament de tòners i demés consumibles es proactiva, en base a sistemes que monitoritzan el consum de forma automàtica.

Manteniment preventiu i correctiu per a garantir les perfectes condicions del parc. El manteniment correctiu cobreix totes les incidències i reparacions que es produeixin als equipaments.

Monitoritzacio dels equips d'impressió i seguiment de les impressions per equip.

Disposem de tres models de tipus d'impressora

Model A : impressora amb blanc i negre , petita per consultoris

Model B : impressora multifunció blanc i negre per cada planta

Model C : impressora multifunció color per administració i residencia

Inventari

	Plantes HOSPITAL							RESIDENCIA	TOTALS
	0	-1	1	2	3	4	5		
Model A	20	7	3	4	7	1	2	3	47
Model B	2	2	1	3	1	1	2	1	13
Model C							1	1	2

Volum mensual d'impressions

Volum mensual pag. promig	
Blanc i negre	55.000
Blanc i negre multifunció	25.000
Color	3.000

PROGRAMARI

Descripció Programari

El His de l'hospital es el programa Savac, esta pendent de evolució a MIRA, pròximament. Amb aquest funciona tota la part assistencial i administrativa,Historia clínica, dades administratives dels pacients, proves radiològiques i de laboratori, farmàcia i prescripció mèdica, compres i magatzem també.

L'Hospital comparteix informació a traves del Nus sanitari amb la Historia clínica compartida de Catalunya, publica informació i consulta informació d'altres Hospitals públics

També s'envia informació al Cat Salut sobre proves que entren en Llistes d'espera i CMBD Conjunt mínim bàsic de dades

esta integrat amb varis programes :

- Anatomia Patològica, rep directament del laboratori extern els resultats de AP i els envia a Historia compartida de Catalunya (HC3).
- Laboratori, les peticions de laboratori les realitza un programa de Sunset que extreu els demogràfics del pacients de savac , ho envia al programa Infinity (Laboratori) , i una vegada fetes les analítiques aquestes es retronen a savac i també s'envien (sunset) a HC3.
- Radiologia , les imatges radiològiques s'envien a HC3 a traves de Sunset.
- Recepta electrònica (Sunset)
- Recordatori de cites als pacients SMs (Alhora)
- Integració amb programa ECAP de ACUT (primaria)
- Integració amb EPAT (triatge d'urgencies)

HOSPITAL COMARCAL SANT BERNABÉ

Historia Clínica compartida de Catalunya

HC3

El HIS de la Residencia es Aegerus i Aegerus SAD (cuidadores a domicili).

A part, hi han els software departamentals que es llisten a continuació (alguns desenvolupats pel propi departament)

- Laboratori : Infinity (Roche), integració peticions a savac(Sunset)
- Recursos humans: Denario (Denario)
- Sistemes : GLPI, zabbixprogrames de desenvolupament Web(Django, Html,PHP) , Drupal , QliKView, Taiga, Alfresco, Mantis BT..
- Comptabilitat : Dimoni
- Documentació : CMBD i llistes d'espera (Costaisa), Iassist
- Formació: plataforma de formació d'althaia
- Bugaderia residencia: Automatització (Logifitd)
- Recepta electrònica : Integració savac (Sunset)
- Publicació imatge digital a HCCC: Integració (Sunset)
- Enviament missatgeria SMS savac recordatori de cites : integració (Alhora)

L'equip del ACUT que fa guàrdies a urgències utilitzen el seu propi programa ECAP amb una integració a savac.

Programes desenvolupats pel departament de sistemes

- Gestió de reclamacions al departament de Unitat d'atenció al client
- Gestió de SEM
- Gestió de manteniment
- Banc d'ajudes tècniques (Residencia)
- Pagina WEB i intranet : amb Drupal

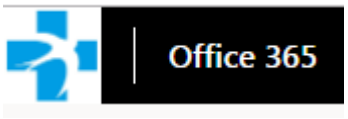
La llista no inclou programari ofimàtica com office, 7zip, pdfcreator etc... que també s'utilitza

Correu Electronic

El correu Electronic esta contractat amb Telefónica, son comptes de correu de Office 365 de 2 categories :

Exchange online Plan 1 pels directius, 19 llicencies (permet replicació amb outlook micrososft 2007 SP2)

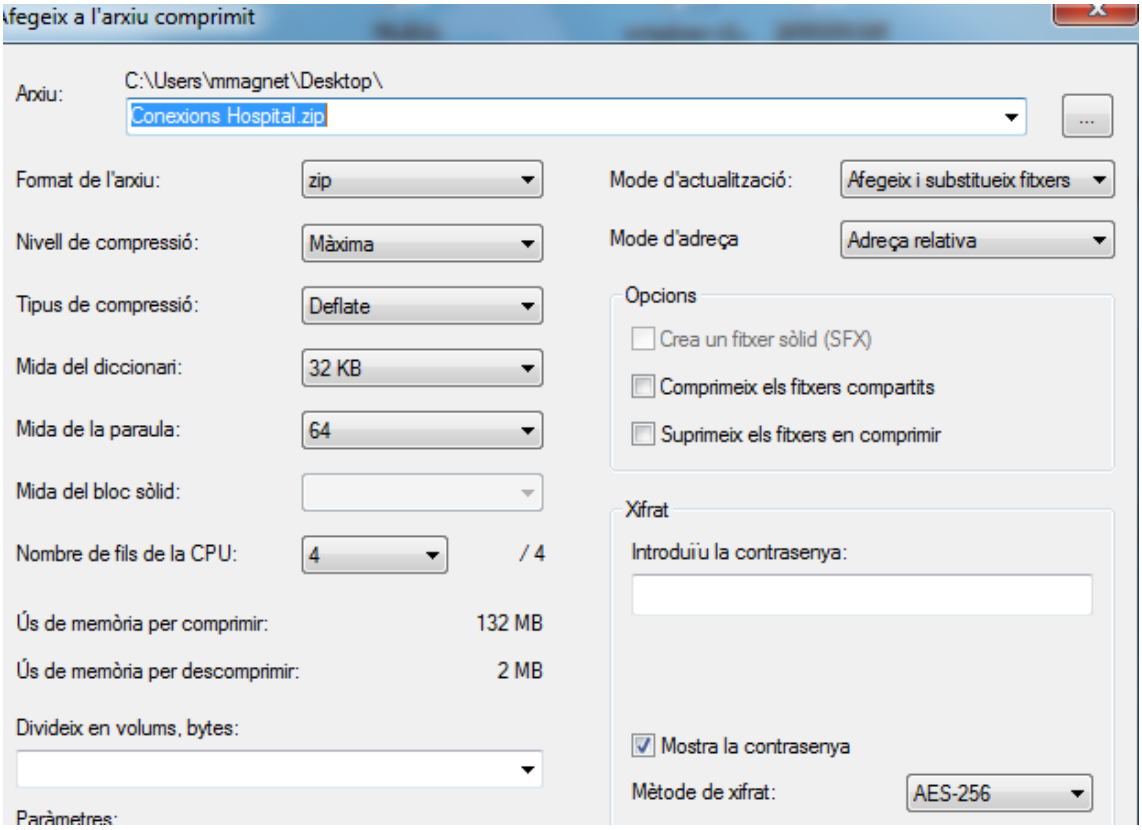
Exchange online 118 llicencies pels professionals



Nombre	Válidas	Expiradas	Asignadas
Exchange Online (plan 1)	19	0	19
Office 365 Empresa	2	0	2
Office 365 Empresa Essentials	1	0	1
Quiosco de Exchange Online	119	0	118

Si cal encriptar informació, s'utilitza 7zip (AES 252) , o Pdfcreator programes gratuïts

IL·LUSTRACIÓ 33 7ZIP



TELEFONIA MOBIL

La fundació disposa de telèfons mòbils pel personal de guàrdia alguns nomes veu i altres amb veu i dades (directius) contractats amb Movistar, ja que es la empresa que ofereix millor cobertura en aquesta zona del Berguedà.

PROJECTES PENDENTS

Control cuidadores domiciliaries (Residencia)

Seran necessaris mòbils per un servei que es dona des de la Residencia i que pròximament s'automatitzarà, el control del desplaçament de les cuidadores a Domicili. Rebran en el mòbil un llistat de pacients i tasques que s'han de realitzar i al arribar i marxar del domicili del pacient podran marcar horari (control amb etiqueta NFC) i tasques realitzades.

Canvi a Telefonia IP

Un dels altres projectes que assumirà pròximament el departament serà el canvi de la centraleta telefònica per una de veu IP.

Admissió automàtica

Un altre projecte pendent es l'admissió automàtica del pacient sense necessitat de passar pel taulell d'admissions.

Renovació de l'electrònica de xarxa i Wifi

Cal renovar tota l'electrònica de xarxa, eliminar miniswitch en alguns punts i cablejar i canviar el sistema wifi. S'està fent un estudi del projecte

Annexa 3. La Informació a la Fundació

LA INFORMACIÓ

La Informació a la Fundació

Tipus d'informació

Dades de Pacients

Dades de Pacients, administratives i sanitàries englobades en la Historia clínica del pacient i en els programes SAVAC a l'hospital i Aegerus a la Residencia.

Les utilitzen el personal administratiu, les que son purament administratives en el departament de administració i facturació i les dades sanitàries de la Història clínica que utilitzen el personal sanitari, metges, infermeria, psicòlegs, assistents socials i altre personal sanitari com rehabilitadors, optometristes etc..

En aquest cas un gran volum de departaments intervenen, mèdics , infermeria, Assistents socials, secretaria mèdica, rehabilitació, Laboratori, radiologia, farmàcia, ...

Dades del personal

Dades del personal (treballadors de la fundació), administratives i de salut que es troben en el programa DENARIO i que utilitza el departament de recursos Humans i Salut Laboral, com contractes, currículums

Dades de la Fundació

Dades de la Fundació com, documents legals, documents de compres i adquisicions, documents de expedients , factures, albarans, ...en el departament de Comptabilitat,compres, secretaria tècnica,

Els programa utilitzat per comptabilitat es el Dimoni

Aquestes dades i la seva seguretat estan garantides en un anterior pla de seguretat fet l'any 2011 seguin la llei aplicable aquell any LOPD, i redactada pel la comissió de seguretat , concretades en varis documents que s'exposaran mes endavant. Es a partir de la revisió d'aquesta documentació i de la actualització de la mateixa a les noves infraestructures i normatives actuals que ha de poder materialitzar-se el nou pla de seguretat.

Bases de dades

Les bases de dades amb informació rellevant segons la anterior son:

DENARIO , dades de treballadors (SQL)

SAVAC, dades mèdiques (ORACLE)

PACS, imatges radiologia (SQL)

DIMONI, dades comptabilitat(SQL)

AEGERUS, dades de residents (MySQL)

UAC , dades de reclamacions (MySQL)

Infinity, Laboratori (cachè)

BAT, (MySQL)

Costaisa, CMBD (SQL)

Recepta electrònica (MySQL)

Responsable dels fitxers

El responsable dels fitxers és l'entitat, representat pel seu Gerent, qui decideix sobre la finalitat, el contingut i l'ús del tractament dels fitxers de dades de caràcter personal de l'Entitat

Documents de seguretat

Documentació existent a la Fundació sobre seguretat de la informació

Trobem 5 documents basics de seguretat:

On hi podem llegir, cito textualment

OBJECTE

L'objectiu d'aquests documents de seguretat és establir les mesures, normes i procediments que afecten als fitxers automatitzats, en paper, o en qualsevol altre suport, llocs de treball, equips, sistemes i programes que intervenen en el tractament de les dades de l'Hospital comarcal Sant Bernabé i la Residència Sant Bernabé (d'ara en endavant l'Entitat), per tal de garantir la seva seguretat, confidencialitat, disponibilitat, fiabilitat i integritat i fer-ho d'acord a la normativa de referència

REFERÈNCIES LEGALS

En compliment de l'establert a la Llei Orgànica 15/ 1999, de 13 de desembre, de protecció de dades de caràcter personal i del Reglament que desenvolupa aquesta Llei Orgànica, concretament el Reial Decret 1720/ 2007 de 21 de desembre (BOE de 19 de gener de 2008), el presents documents de seguretat constitueixen una normativa interior d'obligat compliment per tot el personal de l'entitat, a partir de la data de la seva aprovació.

Igualment aplicable la normativa sectorial a l'efecte, Codi Tipus de la Unió Catalana d'Hospitals, Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent a la salut i l'autonomia del pacient, i la documentació clínica; i Llei 41/2002, de 14 de novembre, bàsica reguladora de la autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.

Document de Seguretat administració

El conjunt de camps de dades que conté el fitxer ADMINISTRACIO és el que es detalla a continuació:

- Dades identificatives
- Nom i cognoms

- Adreça
- Telèfon
- DNI /NIF/NIE
- email

- Dades econòmiques i financeres

Finalitat i usos del fitxer.

La finalitat del fitxer és la gestió econòmica de l'Hospital Comarcal de Sant Bernabé. Els usos són els derivats de realitzar els processos habituals de gestió d'administració, comptabilitat, compres i magatzem.

Determinació del nivell de seguretat aplicable al fitxer

Atesa la tipologia de les dades contingudes en el fitxer i d'acord amb el que disposa el R. D. 1720/2007, de 21 de desembre (en especial, arts.80 i següents) li correspon el nivell de seguretat bàsic.

.....

Legalització del fitxer

El fitxer ha estat enregistrat al Registre de Protecció de Dades de Catalunya de l'Autoritat Catalana de Protecció de Dades en data 21 de juny de 2012 amb el codi 212095008-W. Es pot consultar l'Annex 1. Fitxers inscrits per veure la resolució de l'Autoritat Catalana de Protecció de Dades.

a continuació el documents descriu

Estructura del fitxer

2.1 Suport i sistemes d'informació

2.2 Legalització del fitxer

2.3 Legitimació per al tractament de les dades

2.4 Col·lectiu afectat

2.5 Accés i manteniment de les dades en el fitxer

3. Àmbit d'aplicació del document de seguretat

3.1 Àmbit objectiu

3.2 Àmbit subjectiu

3.3 Àmbit material

4. Organització de la seguretat

Annex 11. Procediment reciclatge suports

Annex 12. Relació d'usuaris amb accés al fitxer

Document de Seguretat de pacients

1. Dades principals del fitxer

1.1 Dades contingudes.

El conjunt de camps de dades que conté el fitxer PACIENTS és el que es detalla a continuació:

Dades identificatives i personals

- Nom i cognoms
- Sexe
- Estat Civil
- Nacionalitat
- Lloc i data naixement
- Adreça
- Telèfon
- DNI /NIF/NIE
- Número d'Afiliació a la Seguretat Social

Dades de salut

- Informes mèdics.
- Diagnòstics i tractaments.
- Curs clínic.
- Constants.
- Prescripció mèdica.
- Tasques i valoracions d'infermeria.
- Serveis de rehabilitació.

Dades socials

- Reconeixements de disminucions.
- Usuari de serveis socials.
- Actitud de la família amb el pacient.
- Activitats en el temps lliure.

1.2 Finalitat i usos del fitxer.

Garantir el registre i seguiment del tractament mèdic, sanitari, soci- sanitari i social que els centres donen a les seves persones usuàries, pacients o residents, així com el continuum assistencial de les persones pacients ateses.

Facilitar informació per a la facturació del servei prestat i l'obtenció d'informació per complimentar la història clínica del pacient.

Servir com a font d'informació necessària per a processos de salut pública, gestió i control sanitari, planificació sanitària, estudis epidemiològics, estadístiques, investigació o docència. D'acord amb allò que preveu l'article 11.3 de la Llei 21/ 2000, de 29 de desembre, sobre els drets d'informació concernent a la salut i l'autonomia del pacient, i la documentació clínica, l'ús amb finalitats epidemiològiques, d'investigació i docència obliga a preservar les dades d'identificació personal de la persona pacient separades de les de caràcter clínic assistencial, llevat que aquesta n'hagi donat el consentiment.

1.3 Determinació del nivell de seguretat aplicable al fitxer

Atesa la tipologia de les dades contingudes en el fitxer i d'acord amb el que disposa el R. D. 1720/2007, de 21 de desembre (en especial, arts.80 i següents) li correspon el nivell de seguretat alt.

AGENCIA DE PROTECCIÓN DE DATOS

/D 60757/2002

HOSPITAL SANT BERNABE
CR RIBES S/N 0 -
08600 BERGA
BARCELONA

Nº Reg. Salida: 60757/2002

El Director de la Agencia de Protección de Datos, a propuesta del Registro General, ha acordado en virtud de las competencias que le atribuyen el art. 12.2.a del Real Decreto 428/1993 de 26 de marzo y el art.7 del Real Decreto 1332/1994 de 20 de junio, vigentes de conformidad con lo dispuesto en la Disposición Transitoria Tercera de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, proceder a la inscripción del fichero notificado con nombre PACIENTES y asignarle el código de inscripción nº 2022670190.

inscripció del fitxer de PACIENTS

Document de seguretat de queixes reclamacions i suggeriments

1.1 Dades contingudes.

El conjunt de camps de dades que conté el fitxer QUEIXES és el que es detalla a continuació:

Dades identificatives i personals

- Nom i cognoms
- Sexe
- Estat Civil
- Nacionalitat
- Lloc i data naixement
- Adreça
- Telèfon
- DNI /NIF/NIE
- Número d'Afiliació a la Seguretat Social

Dades de salut

- Informes mèdics.
- Diagnòstics i tractaments.
- Curs clínic.
- Constants.
- Prescripció mèdica.
- Tasques i valoracions d'infermeria.
- Serveis de rehabilitació.
- Dades socials
- Reconeixements de disminucions.

Usuari de serveis socials.

- Actitud de la família amb el pacient.
- Activitats en el temps lliure.

1.2 Finalitat i usos del fitxer.

Garantir el registre i seguiment de les comunicacions dels usuaris amb la Unitat d'Atenció al Client pel que fa a Queixes, reclamacions, suggeriments i peticions d'atenció.

1.3 Determinació del nivell de seguretat aplicable al fitxer

Atesa la tipologia de les dades contingudes en el fitxer i d'acord amb el que disposa el R. D. 1720/2007, de 21 de desembre (en especial, arts.80 i següents) li correspon el nivell de seguretat alt.

a partir d'aquí s'estructuren els següents apartats

Estructura del fitxer

2.1 Suport i sistemes d'informació

2.2 Legalització del fitxer

2.3 Legitimació per al tractament de les dades

2.4 Col·lectiu afectat

2.5 Accés i manteniment de les dades en el fitxer

3. Àmbit d'aplicació del document de seguretat

3.1 Àmbit objectiu

3.2 Àmbit subjectiu

3.3 Àmbit material

4. Organització de la seguretat

4.1 Responsable del fitxer

4.2 Responsable de seguretat

4.3 Usuaris

4.4 Encarregat de tractament

5. Definició de les normes i procediments de seguretat

5.1 Control d'accés. Relació dels usuaris autoritzats a l'accés a les dades

5.2 Descripció de les funcions i obligacions dels usuaris i tercers amb accés a les dades

Annex 18. Disposició reguladora dels fitxers

Annex 19. Document informatiu sobre la utilització de dades personals

Annex 20. Polítiques de contrasenyes

Annex 21. Personal autoritzat per rebre/enviar documentació/suports amb dades de caràcter personal

Annex 22. Procediment d'encriptació de documents

Annex 23. Claus mestres

Annex 24. Contracte encarregat del tractament

Annex 25. Dret de queixa

Document de seguretat de treballadors

1. Dades principals del fitxer

1.1 Dades contingudes.

El conjunt de camps de dades que conté el fitxer TREBALLADORS és el que es detalla a continuació:

Dades identificatives

- Nom i cognoms
- Sexe
- Estat Civil
- Nacionalitat
- Lloc i data naixement
- Adreça
- Telèfon
- DNI /NIF/NIE
- Número d'Afiliació a la Seguretat Social

- Imatge
- Dades acadèmiques i professionals
- Formació
- Titulacions
- Experiència professional

Dades d'ocupació

- Cos i escala
- Categoria i grau
- Història de la persona treballadora
- Dades d'afiliació sindical
- Dades econòmiques, bancàries i de nòmina
- Dades de circumstàncies socials

1.2 Finalitat i usos del fitxer.

La finalitat és gestionar el personal de l'entitat. Els usos previstos són els derivats de realitzar els processos habituals de gestió de recursos humans, vigilància de la salut i prevenció de riscos laborals del personal.

1.3 Determinació del nivell de seguretat aplicable al fitxer

Atesa la tipologia de les dades contingudes en el fitxer i d'acord amb el que disposa el R. D. 1720/2007, de 21 de desembre (en especial, arts.80 i següents) li correspon el nivell de seguretat alt.

a partir d'aquí s'estructuren els següents apartats

Estructura del fitxer

2.1 Suport i sistemes d'informació

2.2 Legalització del fitxer

2.3 Legitimació per al tractament de les dades

2.4 Col·lectiu afectat

2.5 Accés i manteniment de les dades en el fitxer

3. Àmbit d'aplicació del document de seguretat

3.1 Àmbit objectiu

3.2 Àmbit subjectiu

3.3 Àmbit material

Annex 9. Registre d'entrades i sortides

Annex 10. Usuaris amb accés remot

Annex 11. Procediment reciclatge suports

Annex 12. Relació d'usuaris amb accés al fitxerAnnex

Annex 13. Protocol destrucció paper

Annex 14. Còpies de seguretat

Annex 15. Inventari de suports

Annex 16. Acta de constitució comissió de seguretat

Annex 17. Esquema de servidors i emmagatzemament

Annex 18. Disposició reguladora dels fitxers

Annex 19. Polítiques de contrasenyes

Annex 20. Personal autoritzat per rebre/enviar documentació/suports amb dades de caràcter personal

Annex 21. Procediment d'encriptació de documents

Annex 22. Pla de contingència

Document de seguretat de videovigilancia

HOSPITAL COMARCAL SANT BERNABÉ	DOCUMENT DE SEGURETAT **Nivell de Seguretat Bàsic** **DS - Fitxer de Videovigilància**	Versió:1 Pàgina 1 de 23 Data: 15/11/2013

Objecte

L'objectiu d'aquest document de seguretat és establir les mesures, normes i procediments que afecten als fitxers de l'Hospital comarcal Sant Bernabé i la Residència Sant Bernabé (d'ara en endavant l'Entitat) que tractin dades personals recollides a través d'imatges de persones físiques identificades o identificables, amb finalitats de vigilància mitjançant sistemes de càmeres i càmeres de vídeo, com els noms i cognoms dels visitants al recinte, per tal de garantir la seva confidencialitat, disponibilitat, fiabilitat i integritat.

Referències legals

En compliment de l'establert a la Llei 15/1999 del 13 de desembre de Protecció de Dades Personals i a la Instrucció 1/2009, de 10 de febrer, de l'APDCAT sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància, el present document de seguretat constitueix una normativa interior d'obligat compliment per tot el personal de les entitats, a partir de la data de la seva aprovació.

Desenvolupament

1. Dades principals del fitxer

1.1 Dades contingudes.

En virtut del que estableix l'art. 3 de la Llei Orgànica 15/1999 i l'art. 5.f) del Reial Decret 1720/2007, es considera com a dada de caràcter personal la informació gràfica o fotogràfica.

El tractament de les dades personals obtingudes d'imatges de persones físiques identificades o identificables amb finalitats de vigilància gràcies a sistemes de càmeres o càmeres de vídeo comprendrà l'enregistrament, captació, transmissió, conservació i emmagatzematge d'imatges, inclosa la reproducció o emissió en temps

real, així com el tractament que resulti de les dades personals relacionades amb aquestes imatges i la utilització de qualsevol mitjà anàleg.

En tot cas, les imatges només seran tractades quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades que hagin justificat la instal·lació de les càmeres i càmeres de vídeo, instal·lació que tan sols serà admissible quan la finalitat de vigilància no es pugui obtenir mitjançant altres mecanismes que, sense exigir esforços desproporcionats, resultin menys intrusius per a la intimitat de les persones i per al seu dret a la protecció de dades de caràcter personal.

1.2 Finalitat del fitxer.

El Fitxer de Videovigilància i control d'accés de l'entitat és destinat a preservar el control i la seguretat de l'accés a l'edifici o edificis que formin part de les dependències que són titularitat de l'entitat.

1.3 Usos i aplicacions del fitxer.

Les dades del Fitxer de Videovigilància i Control d'accés són manipulades per l'entitat, únicament per a satisfer les funcions de control i seguretat, però hauran de ser cancel·lades en el termini màxim d'un mes des de la seva captació.

1.4 Deure d'informació.

El Responsable del Fitxer haurà de complir amb el deure d'informació que es preveu a l'art.5 LOPD i concretament:

Haurà de col·locar, en les zones vigilades per vídeo, almenys un distintiu de caire informatiu que s'ubiqui en un lloc que sigui suficientment visible, tan pel que fa a espais oberts com tancats, que haurà de contenir la inscripció "zona videovigilada, Llei Orgànica 15/1999 de Protecció de Dades. Pot exercir els seus drets davant L'Hospital Comarcal de Sant Bernabé" segons el model normalitzat

Tenir a disposició dels interessats impresos, en els que es detalli la informació prevista en l'art. 5.1 LOPD, és a dir:

Existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.

Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.

De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.

De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.

De la identitat i la direcció del responsable del tractament o, si s'escau, del seu representant.

1.5 Determinació del nivell de seguretat aplicable al fitxer

Atenent a la tipologia de les dades contingudes en el fitxer, es determina que li correspon el nivell de seguretat bàsic.

a partir d'aqui

2. Estructura del fitxer i descripció dels suports amb el que està tractat.

3. Àmbit d'aplicació del document de seguretat.

4. Personal afecte al document de seguretat.

5. Manual de funcions.

5.1 El responsable del fitxer.

5.2. Definició de les normes i procediments de seguretat.

5.3 Cessió a tercers de dades de caràcter personal

5.4. Registre d'incidències

5.5. Registre de suports

6. Exercici i tutela dels drets dels afectats.

6.1. Dret d'accés, rectificació, cancel·lació i oposició

9. Annexes

Annex 1. Fitxers inscrits

Annex 2. Model normalitzat i implementat per la comunicació pública d'àrea de zona video vigilada

Annex 3. Còpia del document d'informació i compromís de confidencialitat formalitzat amb usuaris amb accés a aquestes dades

Annex 4-5-6. Model per a l'exercici dels drets d'accés, consulta i cancel·lació de dades

Annex 7. Còpia del document formalitzat amb proveïdors de serveis que tenen o poden tenir la consideració d'encarregat del tractament per disposar d'accés a aquestes dades i/o informacions

Annex 8. Model de document per a registre d'incidències

Annex 9. Model de document informatiu videovigilància

Annex 10. Mapa de situació de les càmeres

Annex 11. Diagrama de xarxa

Annex 12. Protocol còpies de seguretat

Annex 13. Llistat encarregats del tractament

Annexa 4 Abast del SGSI

Objectiu, abast i usuaris

L'objectiu d'aquest document és definir clarament els límits del Sistema de gestió de seguretat de la informació (SGSI) en La Fundació Hospital Sant Bernabé.

Aquest document s'aplica a tota la documentació i activitats dins del SGSI.

Els usuaris d'aquest document són els membres de la direcció de La Fundació Hospital Sant Bernabé, els membres de l'equip del projecte que implementa l'SGSI i el comitè de seguretat de la Fundació.

Definició de l'abast del SGSI

L'organització necessita definir els límits del SGSI per decidir quina informació vol protegir. Aquest tipus d'informació ha de ser protegida independentment de si a més és emmagatzemada, processada o transferida dins o fora de l'abast del SGSI.

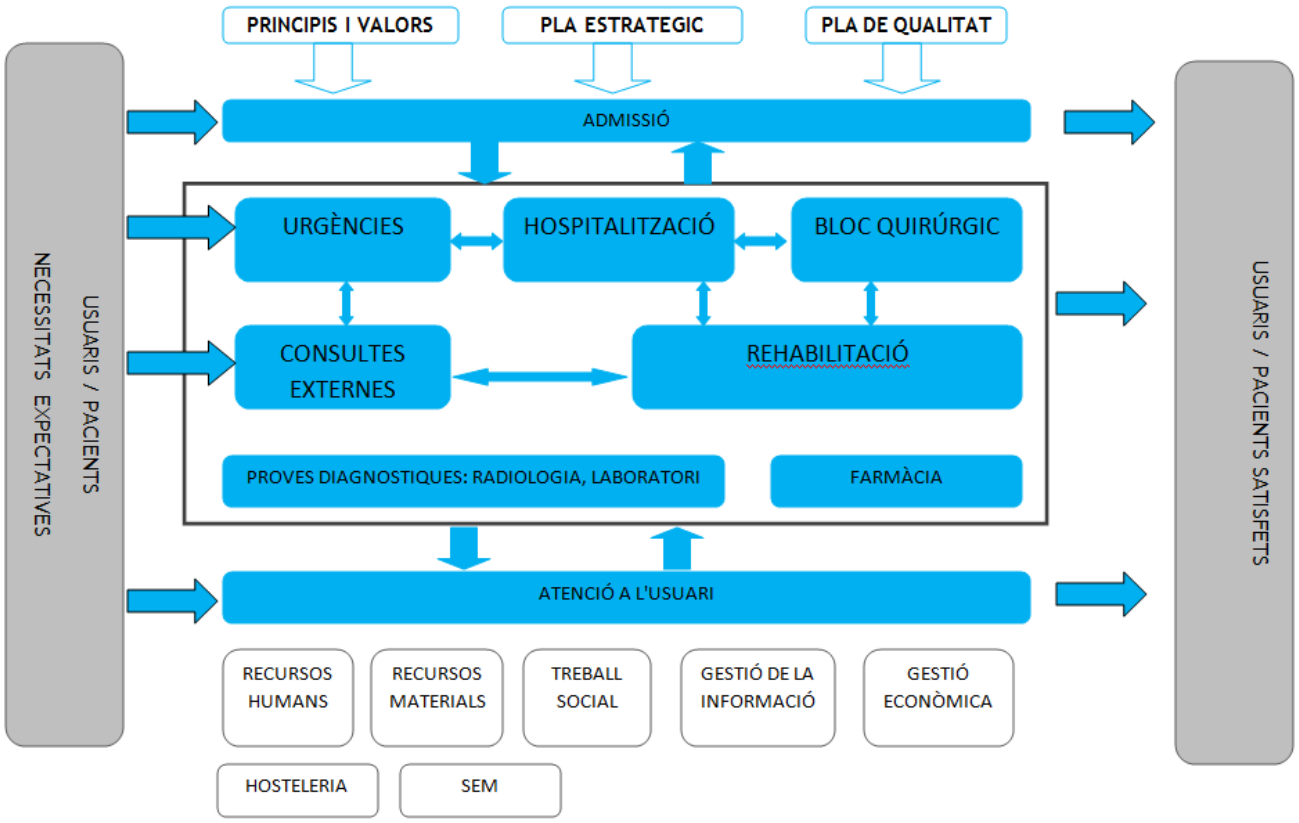
El fet que determinada informació estigui disponible fora de l'abast no vol dir que no se li aplicaran les mesures de seguretat; això només implica que la responsabilitat per l'aplicació de les mesures de seguretat seran transferides a un tercer que administri aquesta informació.

Tenint en compte els requisits legals, normatius, contractuals i d'una altra índole, l'abast del SGSI es defineix d'acord amb els següents aspectes:

- Processos i serveis
- Unitats organitzatives
- Ubicacions
- Xarxes i infraestructura de TI

Processos i serveis

Processos del Hospital



S'inclouen en aquest Pla de seguretat

Tots els processos que abasten la realització de la Historia Clínica del pacient Hospitalari i del Pacient /usuari de la residencia i la gestió de les dades administratives.

Els processos que inclouen dades del personal, tan de gestió de recursos humans com de salut laboral.

La informació que genera la gestió econòmica i legal de la fundació.

Els arxius que contenen informació de la gestió del coneixement i de la comunicació.

S'exclouen els processos que abasten la Hosteleria (menjador neteja) i servei religiós.

Unitats organitzatives, s'inclouen, totes les unitats de caire assistencial i de suport a aquest:

Mediques

- Infermeria
- Laboratori
- Radiologia
- Farmàcia
- Treball social
- Salut Laboral
- Secretaria Mèdica
- Admissions
- Arxiu
- Documentació

Unitats de gestió dels recursos humans:

- RRHH
- Formació

Unitats de gestió administrativa i material:

- Compres
- Comptabilitat
- Facturació
- Magatzem
- Secretaria de direcció
- Secretaria Tècnica
- Manteniment

S’exclouen les unitats de menjador, neteja, servei religiós

ubicacions

Espais que per albergar físicament els mitjans amb què es tracten les dades, i aquells que serveixen directa o indirectament per a accedir al/s fitxer/s.

Són recursos protegits:

- Centres de processament de dades
  - CPD 1 Hospital
  - CPD 2 Hospital
  - CPD 3 Residencia
- Armaris de distribució de xarxa (7)
- 3 Edifici Hospital vell
- 4 Edifici Hospital nou
- 1 Residencia

Tots Llocs de treball, des de els que és te accés als fitxers,

- Consultoris
- Despatxos
- Arxius
- Quiròfans

Xarxes i infraestructura de TI

- Electrónica de xarxa , Switchs
- Cablejat de xarxa coure i fibra, Hospital i Residencia
- Firewalls (3)
- Routers
- ADSL Hospital
- ADSL Residencia
- Fibra Residencia - Hospital
- Fibra Nus Sanitari
- Fibra Internet
- Router TAC
- Pc clients propietat de La fundació, propietat de Althaia (servei de dial.lisis) propietat de ISS
- Servidors
- Cabines d’ emmagatzemen

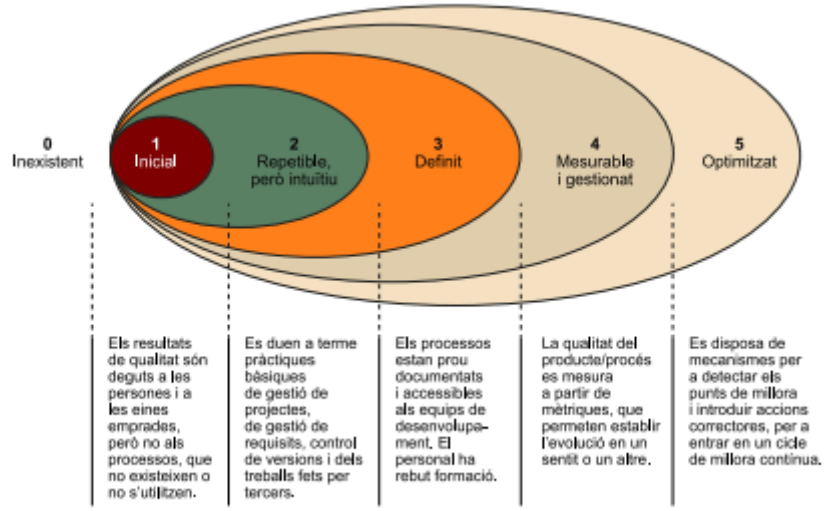
- Mitjans extraïbles
- Impressores
- Aparells electromedicina
- Telèfons mòbils

S'exclou el ADSl del menjador propietat de l'empresa ISS .

Exclusions de l'abast

Com s'ha comentat en punts anteriors s'exclouen tots els actius que pertanyen a la Hosteleria (menjador neteja) i servei religiós menys el PC propietat de ISS connectat a la nostra xarxa interna.

Annexa 5 Anàlisi de Compliment inicial



Els nivells de maduresa del CMM

Percentatge	Nivell
0%	Inexistent
10%	Inicial
50%	Reproduïble, però intuïtiu
90%	Procés definit
95%	Gestionat i Mesurable
100%	Optimitzat

Figura 7: Nivells

Anàlisi de Compliment inicial	%
control Implantació	
5. POLÍTIQUES DE SEGURETAT.	50
5.1 Directrius de la Direcció en seguretat de la informació.	50
5.1.1 Conjunt de polítiques per a la seguretat de la informació.	90
5.1.2 Revisió de les polítiques per a la seguretat de la informació.	10
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	69
6.1 Organització interna.	88
6.1.1 Assignació de responsabilitats per a la segur. de la informació.	95
6.1.2 Segregació de tasques.	95

6.1.3 Contacte amb les autoritats.	100
6.1.4 Contacte amb grups d'interès especial.	50
6.1.5 Seguretat de la informació en la gestió de projectes.	100
6.2 Dispositius per a mobilitat i teletreball.	50
6.2.1 Política d'ús de dispositius per a mobilitat.	50
6.2.2 Teletreball.	50
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS.	**71,1**
7.1 Abans de la contractació.	70
7.1.1 Investigació d'antecedents.	50
7.1.2 Condicions de contractació.	90
7.2 Durant la contractació.	93,3
7.2.1 Responsabilitats de gestió.	95
7.2.2 Conscienciació, educació i capacitació en segur. de la informac.	95
7.2.3 Procés disciplinari.	90
7.3 Cessament o canvi de lloc de treball.	50
7.3.1 Cessament o canvi de lloc de treball.	50
8. GESTIÓ D'ACTIUS.	**56,1**
8.1 Responsabilitat sobre els actius. 8	80
8.1.1 Inventari d'actius.	90
8.1.2 Propietat dels actius.	90
8.1.3 Ús acceptable dels actius.	90
8.1.4 Devolució d'actius.	50
8.2 Classificació de la informació.	65
8.2.1 Directrius de classificació.	95
8.2.2 Etiquetatge i manipulat de la informació.	50
8.2.3 Manipulació d'actius.	50
8.3 Maneig dels suports d'emmagatzematge.	23,3333
8.3.1 Gestió de suports extraïbles.	10
8.3.2 Eliminació de suports.	50
8.3.3 Suports físics en trànsit.	10

9. CONTROL D'ACCESSOS.	**69,7**
9.1 Requisits de negoci per al control d'accessos.	90
9.1.1 Política de control d'accessos.	90
9.1.2 Control d'accés a les xarxes i serveis associats.	90
9.2 Gestió d'accés d'usuari.	56,6667
9.2.1 Gestió d'altes / baixes en el registre d'usuaris.	90
9.2.2 Gestió dels drets d'accés assignats a usuaris.	90
9.2.3 Gestió dels drets d'accés amb privilegis especials.	90
9.2.4 Gestió d'informació confidencial d'autenticació d'usuaris.	50
9.2.5 Revisió dels drets d'accés dels usuaris.	10
9.2.6 Retirada o adaptació dels drets d'accés	10
9.3 Responsabilitats de l'usuari.	50
9.3.1 Ús d'informació confidencial per a l'autenticació.	50
9.4 Control d'accés a sistemes i aplicacions.	82
9.4.1 Restricció de l'accés a la informació.	90
9.4.2 Procediments segurs d'inici de sessió.	90
9.4.3 Gestió de contrasenyes d'usuari.	90
9.4.4 Ús d'eines d'administració de sistemes.	90
9.4.5 Control d'accés al codi font dels programes.	50
10. XIFRAT.	**50**
10.1 Controls criptogràfics.	50
10.1.1 Política d'ús dels controls criptogràfics.	50
10.1.2 Gestió de claus.	50
11. SEGURETAT FÍSICA I AMBIENTAL.	**86,2**
11.1 Àrees segures.	94
11.1.1 perímetre de seguretat física.	95
11.1.2 Controls físics d'entrada.	95
11.1.3 Seguretat d'oficines, despatxos i recursos.	90
11.1.4 Protecció contra les amenaces externes i ambientals.	95
11.1.5 El treball en àrees segures.	95

11.1.6 Àrees d'accés públic, càrrega i descàrrega.	90
11.2 Seguretat dels equips.	62,7778
11.2.1 Emplaçament i protecció d'equips.	95
11.2.2 Instal·lacions de subministrament.	90
11.2.3 Seguretat del cablejat.	90
11.2.4 Manteniment dels equips.	50
11.2.5 Sortida d'actius fora de les dependències de l'empresa.	50
11.2.6 Seguretat dels equips i actius fora de les instal·lacions.	90
11.2.7 Reutilització o retirada segura de dispositius d'emmagatzematge.	50
11.2.8 Equip informàtic d'usuari desatès.	95
11.2.9 Política de lloc de treball buidat i bloqueig de pantalla.	95
12. SEGURETAT A L'OPERATIVA.	**74,3**
12.1 Responsabilitats i procediments d'operació.	60
12.1.1 Documentació de procediments d'operació.	50
12.1.2 Gestió de canvis.	50
12.1.3 Gestió de capacitats.	50
12.1.4 Separació d'entorns de desenvolupament, prova i producció.	90
12.2 Protecció contra codi maliciós.	78,3
12.2.1 Controls contra el codi maliciós.	50
12.3 Còpies de seguretat.	95
12.3.1 Còpies de seguretat de la informació.	95
12.4 Registre d'activitat i supervisió.	91,25
12.4.1 Registre i gestió d'esdeveniments d'activitat.	90
12.4.2 Protecció dels registres d'informació.	90
12.4.3 Registres d'activitat de l'administrador i operador del sistema.	90
12.4.4 Sincronització de rellotges.	95
12.5 Control del programari en explotació.	90
12.5.1 Instal·lació del programari en sistemes en producció.	90
12.6 Gestió de la vulnerabilitat tècnica.	70
12.6.1 Gestió de les vulnerabilitats tècniques.	50

15. RELACIONS AMB SUBMINISTRADORS.	**72,5**
15.1 Seguretat de la informació en les relacions amb subministradors.	95
15.1.1 Política de seguretat de la informació per subministradors.	95
15.1.2 Tractament del risc dins d'acords de subministradors.	95
15.1.3 Cadena de subministrament en tecnologies de la informació i comunicacions.	95
15.2 Gestió de la prestació del servei per subministradors.	50
15.2.1 Supervisió i revisió dels serveis prestats per tercers.	50
15.2.2 Gestió de canvis en els serveis prestats per tercers.	50
16. GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	95
16.1 Gestió d'incidents de seguretat de la informació i millores.	95
16.1.1 Responsabilitats i procediments.	95
16.1.2 Notificació dels esdeveniments de seguretat de la informació.	95
16.1.3 Notificació de punts febles de la seguretat.	95
16.1.4 Valoració d'esdeveniments de seguretat de la informació i presa de decisions.	95
16.1.5 Resposta als incidents de seguretat.	95
16.1.6 Aprenentatge dels incidents de seguretat de la informació.	95
16.1.7 Recull d'evidències.	95
17. SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.	**80,8**
17.1 Continuïtat de la seguretat de la informació.	66,6667
17.1.1 Planificació de la continuïtat de la seguretat de la informació.	95
17.1.2 Implantació de la continuïtat de la seguretat de la informació.	95
17.1.3 Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	10
17.2 Redundàncies.	95
17.2.1 Disponibilitat d'instal·lacions per al processament de la informació.	95
18. COMPLIMENT.	**83**
18.1 Compliment dels requisits legals i contractuals.	86
18.1.1 Identificació de la legislació aplicable.	95
18.1.2 Drets de propietat intel·lectual (DPI).	95
18.1.3 Protecció dels registres de l'organització.	95
18.1.4 Protecció de dades i privacitat de la informació personal.	95

18.1.5 Regulació dels controls criptogràfics.	50
18.2 Revisions de la seguretat de la informació.	80
18.2.1 Revisió independent de la seguretat de la informació.	95
18.2.2 Compliment de les polítiques i normes de seguretat.	95
18.2.3 Comprovació del compliment	50

*** s'adjunta excel amb les especificacions de la documentació revisada**

Annexa 6 Política de seguretat de la informació

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aprovació I entrada en vigor

Text aprovat el dia _____ pel Comitè de Seguretat. Aquesta Política de Seguretat de la Informació és efectiva des de l'esmentada data i fins que sigui reemplaçada per una nova Política.

1. Introducció

1.1. Missió i serveis prestats

La Fundació Hospital Comarcal de Sant Bernabé és una organització sanitària comarcal que té com a finalitat prestar serveis de salut i atenció a la dependència a la població de la comarca del Berguedà. Té com a valors la professionalitat, el treball en equip, la qualitat i el respecte a les persones. La seva missió és oferir als ciutadans i el seu entorn una atenció sanitària integral, de qualitat, amb continuïtat assistencial entre tots els nivells i centrada en les persones.

Entre d'altres, són competències pròpies del Hospital de la Fundació oferir serveis ambulatoris, de hospitalització i sociosanitaris i de la Residencia serveis de Residència assistida, Acolliment diürn, Programa Descans, Gent Gran a Casa, Serveis d'atenció domiciliària i de Ajudes Tècniques.

Té la consideració d'organisme municipal autònom. El govern, administració i representació de lo Fundació es confia, de manera exclusiva, al Patronat, nomenat amb subjecció al disposat en el seus Estatuts

2.Justificació de la Política de seguretat de la informació

2.1. Necessitat de seguretat en els sistemes

Per al compliment de la seva Missió, la prestació dels Serveis identificats i el compliment dels seus objectius, la Fundació depèn dels sistemes d'informació i les TIC (Tecnologies de la Informació i Comunicacions). Aquests sistemes han de ser administrats amb diligència, i adoptar les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar la confidencialitat, integritat,

disponibilitat, autenticitat i traçabilitat de la informació tractada o dels serveis prestats.

L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb rapidesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, autenticitat, traçabilitat, ús previst i valor de la informació i els serveis.

Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica s'han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (en endavant ENS), així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

L'ENS (Reial Decret 3/2010, de 8 de gener), en el seu article 11 estableix que "Tots els òrgans superiors de les Administracions Públiques hauran de disposar formalment de la seva política de seguretat, que serà aprovada pel titular de l'òrgan superior corresponent ".

2.2. Requisits de seguretat en els Departaments.

Totes les Àrees de la Fundació han d'aplicar les mesures mínimes de seguretat exigides per l'ENS, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats. Els diferents departaments han de assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació.

Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC. Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se de incidents, d'acord amb l'article 7 de l'ENS.

2.3 Lideratge I Compromís de la direcció

La Direcció de La Fundació es compromet a facilitar i proporcionar els recursos necessaris per a l'establiment, implantació, manteniment i millora del SGSI / ENS de l'entitat, així com a demostrar lideratge i compromís respecte a aquest, a través de la constitució del Comitè de Seguretat de la Informació.

3. MARC NORMATIU

3.1 Normativa de caràcter comunitari

•Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la i protecció de les persones físiques paper que fa al Tractament de dades personals i a la lliure Circulació d'aquestes dades i paper qual és deroga la Directiva 95/46 / CE (Reglament general amb protecció de dades)

3.2 Llei estatal

• Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text refós de la llei de propietat intel·lectual.

• Llei 59/2003, de 19 de desembre, de signatura electrònica.

• Llei 56/2007 o Llei per a l'Impuls de la Societat de la Informació.

• Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics, en el seu article 42.2, estableix sobre l'ENS, com un dels seus principis, que s'ha de disposar d'un marc de referència que estableixi les condicions necessàries de confiança en l'ús dels mitjans electrònics.

• Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals

• Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.

3.3 Llei autonòmica

• Llei 26/2010 del 3 d'agost de règim jurídic i Procediment de les Administracions Públiques de Catalunya

• Llei 16/2015 de 21 de juliol de simplificació de l'activitat administrativa de l'Administració de la Generalitat i dels Governs Locals de Catalunya i l'impuls de l'activitat econòmica.

• Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

3.4 Reglaments

• 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.

• Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.

• Reial Decret 704/2011, de 20 de maig, pel qual s'aprova el Reglament de protecció de les infraestructures crítiques.

• Reial Decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

• Reial Decret 3/2010, de 8 de gener (BOE de 29 de gener), pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica. fixa els principis bàsics i requisits mínims, així com les mesures de protecció a implantar en els sistemes de l'Administració

• Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.

• Reial Decret 704/2011, de 20 de maig, pel qual s'aprova el Reglament de protecció de les infraestructures crítiques.

4. ORGANITZACIÓ DE LA SEGURETAT.

4.1 Rols: funcions i responsabilitats.

La Política de Seguretat, segons requereix l'Annex II de l'ENS en la seva secció 3.1, ha d'identificar uns clars responsables per vetllar pel seu compliment i ser coneguda per tots els membres de l'organització administrativa.

S'estableixen els següents rols en l'organització relacionats amb la Seguretat de la Informació.

4.1.2 Responsable de la Informació

Aquestes funcions seran assumides per, la Gerència, en representació del Patronat de la Fundació, aquest entén la missió de la Fundació, determina els objectius que es proposa assolir i respon de que s'aconsegueixin.

Les seves funcions seran les següents:

- Té la responsabilitat última de l'ús que es faci d'una certa informació i, per tant, de la seva protecció.
- És el responsable últim de qualsevol error o negligència que porti a un incident de confidencialitat o d'integritat.
- Estableix els requisits de la informació en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.
- Determinarà els nivells de seguretat en cada dimensió dins el marc establert en l'Annex I de l'ENS.

- Encara que l'aprovació formal dels nivells correspongui al responsable de la Informació, podrà demanar una proposta al responsable de la Seguretat i convé que escolti l'opinió del responsable del Sistema.

4.1.3 Responsable de la seguretat de la informació

Comitè de seguretat: funcions i responsabilitats.

El Comitè de Seguretat de la Informació, és l'òrgan que coordina la Seguretat de la Informació a nivell de la Fundació i es el responsable de aquesta.

Esta constituït :

- Per la Secretaria tècnica,
- La direcció de la Unitat d'atenció a l'usuari,
- El Cap del departament d'Informàtica,
- El Responsable de admissions,
- i per representants de les àrees afectades per l'ENS

Els membres del Comitè de Seguretat de la Informació, son nomenats per la Gerència de la Fundació.

Les funcions del comitè són les següents:-

- Desenvolupar i mantenir l'estratègia corporativa de protecció
- Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè sigui aprovada per la Direcció.
- Aprovar la normativa de seguretat de la informació.
- Promoure la millora contínua del Sistema de Gestió de la Seguretat de la Informació.
- Atendre les inquietuds de la Corporació i dels diferents departaments.
- Informar regularment l'estat de la seguretat de la informació a l'Alta Direcció.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
- Monitoritzar els principals riscos residuals assumits per l'Organització i recomanar possibles actuacions respecte d'ells.
- Monitoritzar l'acompliment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'ells.

- Coordinació les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.
- Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Analitzar els informes d'Auditoria .
- Aprovar plans de millora de la seguretat de la informació de l'Organització.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i / o entre diferents àrees de l'Organització, elevant aquells casos en què no tingui prou autoritat per decidir.
- Exigir el compliment de les condicions de seguretat a tots nivells quan el tractament el realitzi un tercer, mitjançant l'elaboració de compromisos legals amb els encarregats externs de tractament.

El Comitè de Seguretat de la Informació no és un comitè tècnic, ha de demanar regularment del personal tècnic propi o extern, la informació pertinent per prendre decisions.

El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els quals hagi de decidir o emetre una opinió.

Aquest assessorament es determinarà en cada cas, podent materialitzar de diferents formes i maneres:

- Grups de treball especialitzats interns, externs o mixtes.
- Assessoria externa.

Assistència a cursos o un altre tipus d'entorns formatius o d'intercanvi d'experiències.

4.1.4 Responsables de departaments

Els responsables de departaments, enténen què fa cada departament, i com es coordinen entre si per assolir els objectius marcats per la Direcció.

Funcions associades en quant a la seguretat

- Té la potestat de determinar els nivells de seguretat dels serveis dins el marc establert en l'Annex I de l'ENS.
- Té la responsabilitat última de l'ús que es faci de determinats serveis i, per tant, de la seva protecció. -

- És el responsable últim de qualsevol error o negligència que porti a un incident de disponibilitat dels serveis que gestiona.
- Encara que l'aprovació formal dels nivells correspongui al Responsable del Servei, podrà demanar una proposta al comitè de Seguretat i convé que escolti l'opinió del responsable de Tecnologies.

4.1.5 Responsable de Sistemes i de les tecnologies de la Informació (CIO)

Serà exercit pel Cap del Departament d'Informàtica, CIO

Les seves funcions seran les següents:

- Coordinar les necessitats de Seguretat de la Informació en el marc de la resta de necessitats de Seguretat Corporativa.
- Mantindrà la seguretat de la informació i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb el que estableix la Política de Seguretat de l'Organització.
- Promourà la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.
- Realitzarà l'Anàlisi de Riscos
- Elaborarà la declaració de Aplicabilitat a partir de les mesures de seguretat requerides d'acord a l'Annex II de l'ENS i del resultat de l'Anàlisi de Riscos.
- Ha de informar al responsable de la informació i al comitè de seguretat del nivell de risc residual esperat, després implementar les opcions de tractament seleccionades en l'anàlisi de riscos i les mesures de seguretat requerides pel ENS.
- Coordinarà l'elaboració de la Documentació de Seguretat del Sistema.
- Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per a la seva aprovació per Direcció.
- Participarà en l'elaboració i aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de Seguretat de la Informació.
- Elaborarà i aprovar els Procediments Operatius de Seguretat de la Informació.
- Ha de facilitar periòdicament al Comitè de Seguretat un resum d'actuacions en matèria de seguretat, d'incidents relatius a seguretat de la informació i l'estat de la seguretat del sistema (en particular del nivell de risc residual a què està exposat el sistema).
- Ha d'elaborar, al costat del Administrador de Sistemes, Plans de Millora de la Seguretat, per la seva aprovació pel Comitè de Seguretat de la Informació.

- Validarà els Plans de Continuïtat de Sistemes que elabori el Administrador de Sistemes, i que ha d'aprovar el Comitè de Seguretat de la Informació i provats periòdicament pel Responsable de Sistemes.
- Aprovarà les directrius proposades pel Administrador de Sistemes per a considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis.
- En cas d'ocurrència d'incidents de seguretat de la informació analitzarà i proposarà salvaguardes que previnguin incidents similars en un futur.
- Planificarà la implantació de les salvaguardes en el sistema

Podrà designar els Delegats que consideri necessaris.

Per mitjà de la designació de Delegats, es delegaran funcions.

La responsabilitat final seguirà recaient sobre el responsable de la Seguretat.

Els delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegui el responsable de sistemes i de les tecnologies de la informació, podent ser, per exemple, la seguretat de sistemes d'informació concrets o de sistemes d'informació horitzontals. Cada responsable de seguretat Delegat tindrà una dependència funcional directa del CIO, que és a qui reporten.

4.1.6 Administrador de Sistemes

El Cap del departament d'informàtica nomenarà formalment al administrador de sistemes , una única persona en l'organització.

Les seves funcions seran les següents:

- La implementació, gestió i manteniment de les mesures de seguretat aplicables als Sistemes d'Informació.
- La gestió, configuració i actualització, si escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat dels Sistemes d'Informació.
- Desenvolupar, operar i mantenir els Sistemes de Informació durant tot el seu cicle de vida, les seves especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i sistema de gestió dels Sistemes d'Informació establint els criteris d'ús i els serveis disponibles en el mateix.
- El Responsable dels Sistemes pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els Responsables de la Informació afectada, del Servei afectat i amb el responsable de la Seguretat abans de ser executada. -

- Monitoritzar l'estat de la seguretat dels Sistemes d'Informació i reportar periòdicament o davant incidents de seguretat rellevants al responsable de Seguretat de la Informació.
- Elaborar els Plans de Continuïtat dels Sistemes perquè siguin validats pel coordinats i aprovats pel Comitè de Seguretat de la Informació.
- Realitzar exercicis i proves periòdiques dels Plans de Continuïtat del Sistema per mantenir-los actualitzats i verificar que són efectius.
- Informar els responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa.

Derivades del comitè de seguretat

- Assegurar-se que les mesures específiques de seguretat s'integrin adequadament dins el marc general de seguretat.
- Assegurar que els controls de seguretat establerts són complerts estrictament.
- Assegurar que la traçabilitat, pistes d'auditoria i altres registres de seguretat requerits es troben habilitats i registrin amb la freqüència desitjada, d'acord amb la Política de Seguretat establerta per l'Organització

En cas d'ocurrència d'incidents de seguretat de la informació:

- Dur a terme el registre i gestió dels incidents de seguretat en els Sistemes sota la seva responsabilitat.
- Executar el pla de seguretat aprovat.
- Aïllar el incident per evitar la propagació a elements aliens a la situació de risc.
- Prendre decisions a curt termini si la informació s'ha vist compromesa de cap forma que pugui tenir conseqüències greus (aquestes actuacions haurien d'estar procedim entades per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Assegurar la integritat dels elements crítics del sistema si s'ha vist afectada la disponibilitat dels mateixos.
- Mantenir i recuperar la informació emmagatzemada pel Sistema i els seus serveis associats.
- Investigar l'incident: Determinar la manera, els mitjans, els motius i l'origen de l'incident.

4.1.7 Responsable de Recursos Humans

Els responsable de recursos humans s'ajustaran al que estableix l'ENS en matèria de personal de manera anàloga al que estableixen els punts anteriors. El responsable de personal implantarà les mesures de seguretat que els competeixin dins de les determinades pel Comitè de Seguretat de la Informació, i informaran aquest del seu grau d'implantació, eficàcia i incidents.

4.1.8 DPD, Delegat de protecció de dades

Segons El Reglament General de Protecció de Dades (UE) 2016/679 (RGPD) de la Unió Europea (article 37) i Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia dels Drets Digitals, (article 34) la nostra Fundació esta obligada a comptar amb un delegat de Protecció de Dades com a centres sanitaris legalment obligat al manteniment de les històries clíniques dels pacients.

El Delegat de protecció de dades supervisa internament, el compliment de les obligacions que imposa el RGPD.

El mateix Reglament exigeix que tal figura tingui garantit un funcionament independent.

El delegat de protecció de dades serà designat atenent les seves qualitats professionals i, en particular, als seus coneixements especialitzats del Dret i la pràctica en matèria de protecció de dades i la seva capacitat per exercir les funcions indicades en l'article 39.

El delegat de protecció de dades podrà formar part de la plantilla del responsable o de l'encarregat del tractament o exercir les seves funcions en el marc d'un contracte de serveis.

El responsable o l'encarregat del tractament publicaran les dades de contacte del delegat de protecció de dades i els comunicaran a l'autoritat de control.

El delegat de protecció de dades té, entre d'altres, les funcions següents:

- Informar i assessorar el responsable o l'encarregat i els treballadors sobre les obligacions que imposa la normativa de protecció de dades.
- Supervisar que es compleix la normativa.
- Assessorar respecte de l'avaluació d'impacte relativa a la protecció de dades.
- Cooperar amb l'autoritat de control.
- Actuar com a punt de contacte per a qüestions relatives al tractament.

4.5. Relació amb el document de seguretat i protecció de dades personals.

Per a la prestació dels serveis de la Fundació han de ser tractats dades de caràcter personal. El Document o documents de Seguretat de la Fundació detallaran els fitxers afectats i els responsables corresponents, així com les mesures adoptades en el marc

del Reial Decret 1720/2007 i normativa complementària. Tots els sistemes d'informació s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollides en l'esmenta't document

5. GESTIÓ DE RISCOS.

5.1. Justificació.

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats. L'anàlisi de riscos serà la base per determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establerts per l'ENS, segons el que preveu l'article 6 del mateix.

5.2. Criteris d'avaluació de riscos

Per l'harmonització de les anàlisis de riscos, el Departament TIC s'establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats. Els criteris d'avaluació de riscos detallats s'especificaran en la metodologia d'avaluació de riscos que elaborarà l'organització, basant-se en estàndards i bones pràctiques reconegudes. En concret, la Fundació efectuarà una anàlisi i avaluació de riscos basant-se en la metodologia MAGERIT V.3

Hauran tractar-se, com a mínim, tots els riscos que puguin impedir la prestació dels serveis o el compliment de la missió de l'organització de forma greu. Es prioritzaran especialment els riscos que impliquin un cessament en la prestació de serveis de salut als ciutadans

5.3. Directrius de tractament

El Comitè de Seguretat dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

5.4. Procés d'acceptació del risc residual

Els riscos residuals seran determinats pel anàlisis del risc.

Els nivells de Risc residuals esperats sobre cada Informació o servei després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II de l'ENS) hauran de ser acceptats prèviament pels responsables corresponents.

Els nivells de risc residuals seran presentats pel Responsable de Tecnologies de Seguretat de la Informació al Comitè de Seguretat de la Informació, perquè aquest procedeixi, si s'escau, a avaluar, aprovar o rectificar les opcions de tractament proposades.

5.5. Necessitat de realitzar o actualitzar les avaluacions de riscos.

L'anàlisi dels riscos i el seu tractament han de ser una activitat repetida regularment, segons el que estableix l'article 9 de l'ENS.

Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada a l'any.
- Quan es produeixin canvis significatius en la informació manejada.
- Quan es produeixin canvis significatius en els serveis prestats.
- Quan es produeixin canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.
- Quan passi un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

6. GESTIÓ D'INCIDENTS DE SEGURETAT.

6.1. Prevenció d'incidents.

Els departaments han d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats

6.2. Monitorització i detecció d'incidents

Per garantir el compliment de la Política, els departaments han de:

- Autoritzar els sistemes abans d'entrar en operació.
- avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració realitzats de forma rutinària.

6.3. Resposta davant incidents.

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una disminució fins al cessament del nivell de prestació, els serveis han de monitoritzar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons que estableix l'article 9 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS.

S'establiran mecanismes de detecció, anàlisi i report que puguin informar els responsables tant regularment com quan es produeixi una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

Les diferents Àrees de la Fundació han de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar punts de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident.

6.4. Recuperació davant incidents i plans de continuïtat.

Per garantir la disponibilitat dels serveis crítics, els departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

7. OBLIGACIONS DEL PERSONAL

Tot el personal de la Fundació, tant empleats com directius, té l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, i és responsabilitat del Comitè de Seguretat disposar els mitjans necessaris perquè la informació arribi als mateixos.

Tot el personal de la Fundació s'haurà de conscienciar en matèria de seguretat TIC com a mínim un cop cada dos anys.

S'establirà un programa de conscienciació contínua per atendre tots els membres de l'organització, en particular als de nova incorporació.

El personal amb responsabilitat en l'ús, operació o administració de sistemes TIC rebrà formació per al maneig segur dels sistemes en la mesura que la necessiti per realitzar-la.

La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

El compliment d'aquesta Política de Seguretat és obligatori per part de tot el personal intern o extern que intervingui en els processos l'organització, constituint el seu incompliment **infracció greu** a efectes laborals.

8. OBLIGACIONS DE TERCERS

Quan la fundació presti serveis o utilitzi informació d'altres entitats, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals per reportar i coordinar els respectius Comitès de Seguretat TIC i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan s'utilitzin serveis externs o se cedeixi informació a entitats o empreses, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que pertoqui a aquests serveis o informació.

Aquesta tercera part quedarà subjecta a les obligacions establertes en l'esmentada normativa, podent desenvolupar seus propis procediments operatius per satisfer-la.

S'establiran procediments específics d'informe i resolució d'incidències.

S'ha de garantir que el personal aliè a aquesta Fundació que hagi d'utilitzar la informació, està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política.

Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del responsable de seguretat que inclourà els riscos en què s'incorre i la forma de tractar-los.

Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant

9. DOCUMENTACIÓ COMPLEMENTÀRIA

La Política de Seguretat de la Informació s'omplirà amb documents més precisos que ajuden a dur a terme el proposat.

Per a això s'utilitzaran:

- Normes de seguretat (security estàndards).
- Guies de seguretat (security guides).
- Procediments de seguretat (security procedures).

Les normes uniformitzen l'ús d'aspectes concrets del sistema. Indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori.

Les guies tenen un caràcter formatiu i busquen ajudar els usuaris a aplicar correctament les mesures de seguretat proporcionant raonaments on no hi ha procediments precisos. Per exemple, com escriure procediments de seguretat. De la

mateixa manera, les guies ajuden a prevenir que es passin per alt aspectes importants de seguretat que poden materialitzar-se de diverses formes.

Els procediments [operatius] de seguretat afronten tasques concretes, indicant el que cal fer, pas a pas. Són útils en tasques repetitives.

La normativa de seguretat estarà a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

Trobem a la Fundació varies Politiques i normes de obligat compliment descrites en un apartat posterior (12)

10. REVISIÓ I APROVACIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ.

La Política de Seguretat de la Informació serà revisada pel Comitè de Seguretat de la Informació i pel DPD a intervals planificats, que no podran excedir 2 anys de durada, o sempre que es produeixin canvis significatius, per tal d'assegurar que es mantingui la seva idoneïtat, adequació i eficàcia.

Els canvis sobre la Política de Seguretat de la Informació les ha d'aprovar l'òrgan superior competent que correspongui, d'acord amb l'article 11 de l'ENS.

Qualsevol canvi sobre la mateixa haurà de ser difós a totes les parts afectades.

11 Registres

Taula de Registres

Els registres d'aquesta política, s'hauran de mantenir durant el temps que resulti exigible per la normativa nacional o comunitària.

12 Històric de modificacions

VERSIÓ /	REVISIÓ	DATA MODIFICACIONS

annexa 50

12. Politiques i normes de la Fundació de obligat compliment

- Procediment, gestió i registre d'incidències
- generació Informe mensual del sistema
- Informació i compromís de l'empleat
- Manual de bones pràctiques
- Compromís de confidencialitat
- Registre d'entrades i sortides
- Usuaris amb accés remot
- Procediment reciclatge suports
- Relació d'usuaris amb accés al fitxer
- Protocol destrucció paper
- Procediments, periodicitat i custòdia per a la realització de còpies de seguretat
- Pla de contingència
- Procediment dissociació HC
- Polítiques de contrasenyes
- Personal autoritzat per rebre/enviar documentació/suports amb dades de caràcter personal
- Document informatiu sobre la utilització de dades personals
- Protocol d'accés a la documentació clínica.
- Personal autoritzat per rebre/enviar documentació/suports amb dades de caràcter personal
- Procediment d'encriptació de documents
- Claus mestres
- Contracte encarregat del tractament
- Control d'accés. Relació dels usuaris autoritzats a l'accés a les dades
- Llista Encarregats de tractament
- Descripció de les funcions i obligacions dels usuaris i tercers amb accés a les dades

- Relació d'usuaris amb autorització per aportar documents a HC Savac
- Personal autoritzat per rebre/enviar documentació/suports amb dades de caràcter personal
- Cessió a tercers de dades de caràcter personal

- Mecanismes de seguretat en la transmissió de la informació
- Proves amb dades reals
- Formalització de registres
- Règim de treball fora dels locals de la ubicació dels Fitxers
- Gestió de suports
- Procediment exercici de drets ARCO
- Dret de queixa
- Aplicabilitat del Document de Seguretat com a Encarregat de Tractament
- Revisió mensual del sistema de protecció de dades
- Legitimació per al tractament de les dades
- Organització de la seguretat
- Responsable del fitxer
- Responsable de seguretat
- Usuaris
- Definició de les normes i procediments de seguretat

Annexa 7 Procediment d'auditories internes

Objectiu de l'auditoria

Aquest procediment te l'objectiu de ser una guia per realitzar periòdicament auditories internes

Auditarà el compliment de la normativa implementada en aquest SGSI , la verificació dels controls que si descriuen ,i la millora continua d'aquest.

Analitzarà aspectes organitzatius tècnics i físics

Responsable

El Responsable de seguretat programarà, organitzarà i vetllarà per que l'auditoria es porti a terme tal com s'ha planificat.

També en son responsables el comitè de seguretat i la direcció.

L'auditoria es portarà a terme en l'Hospital Sant Bernabé i es visitarà també la Residencia Sant Bernabé.

La gerència destinarà la assignació dels recursos i les partides necessàries per dur a terme l'auditoria

Abast:

L'abast de l'auditoria seran els processos, i les infraestructures que abasta el SGSI en especial els mes crítics i els mes vulnerables

Recursos

El personal adscrit al comitè de seguretat juntament el personal de TIC portaran a terme els processos de l'auditoria vetllant per no incomplir la norma de independència en el procés auditat.

Per tan, es formarà si cal, al personal adscrit a cada tasca.

La direcció nomenarà un Auditor Intern, expert.

L'auditor intern deurà posseir alguna titulació relacionada amb la seguretat de la informació

Aquesta persona tindrà les següents funcions i obligacions:

Comprendre i complir amb els criteris per realitzar l'auditoria

Verificar la definició i correcta aplicació dels procediments de l'auditoria

interna

Presentar els informes d'auditoria

Guardar en secret les dades obtingudes al realitzar l'auditoria

Conèixer la normativa interna

Es posarà a disposició de l'equip auditor tota la documentació necessària

Pla de seguretat

Politiques de seguretat

Documents tècnics de les infraestructures auditades

Es faran entrevistes amb el Director de sistemes, amb el de Recursos humans

Fases

Formació dels auditors interns a càrrec de la empresa.

Recol·lecció d'informació prèvia

Execució de les proves d'auditoria

Anàlisi de la informació

Elaboració i presentació de l'informe

Llista detallada de les constatacions

Informe d'auditoria que ha de incloure

Data auditoria

Nom auditors i responsabilitats o càrrecs

Abast , processos, departaments,controls auditats

Grau d'adequació del SGSI amb la norma

No conformitats detectades

Recomanacions de millora si es creu convenient

Planificació

Es dura a terme una vegada a a l'any, i la duració prevista es d'una a dues setmanes

Implementació

L'auditor intern serà el responsable de que es realitzin les tasques d'auditoria i de recopilar els informes , s'auditarà:

- Revisió del compromís de la governança de la seguretat de la informació
- política de seguretat i actualitzacions fetes i si se'n deriva documentació
- política de classificació informació
- actes comitè seguretat
- subcontractació serveis IT

- Revisió de la seguretat física
- Revisió dels tres CPD: subministrament elèctric, tº ,humitat ,extinció incendis accessos
- Revisió armaris rack , subministrament elèctric, pols
- Sala formació comunicació
- procediments d'instal·lació/retirada d'equips
- procediments d'accés a les sales
- revisio SAIS (estat de les bateries)
- Revisió de la seguretat lògica
- Altes /baixes usuaris directori actiu
- Altes /baixes usuaris savac, aegerus
- Altes /baixes usuaris correu
- Assignació de rols
- Politiques contrasenyes i implementació
- Els registres d'accés a dades confidencials
- Pantalles desateses (en un hospital es important no deixar dades de pacients a la vista)
- Antivirus
- Revisió de la seguretat perimetral de les xarxes de comunicacions
- revisió VPN
- wifi
- anàlisis vulnerabilitat, prova d'intrusió
- revisio firewall trafic i regles
- Revisió dels plans de continuïtat de negoci
- Copies de seguretat
- Redundància CPD
- Redundància accés Internet , Residencia (accés a Aegerus)

- Revisió de la capacitat de resposta davant incidents
- revisió del registres d'incidents seguretat
- revisió pla de contingència

Revisió i millora

L'auditoria s'haurà de revisar una vegada feta per implementar solucions a les constatacions trobades

Informe d'auditoria

Haurà d'incloure ,

nom del responsable , objectiu i anàlisis realitzat , conclusions i propostes de millora si cal, nivell de classificació

Exemple :

	Informe d'auditoria - NO CONFORMITAT Objectiu : Revisió de la seguretat física	Data: 21/03/2017
	Actiu: CPD2 , SAI bateries en mal estat ,	Responsable: Montse Magnet
	Proposta millora: cal canviar-les	Nivell : 4

Classificació importància constatacions

ID - Nivell

Nivell :

5-Critic : Resoldre immediatament que sigui possible

4-Important: Resoldre en quant e sigui possible

3-Moderadament important : No ha de ser ignorat ni assumit, s'ha de resoldre

2-Lleugerament important: Es pot esperar a la propera reconfiguració planificada però no ha de ser ignorat ni assumit

1-A títol informatiu : es recomana que es gestioni no que s'ignori o s'assumeixi

Documentació ISO 27001 a revisar anualment

- L'abast del sistema de gestió de seguretat de la informació (clàusula 4.3)
- Política de seguretat de la informació i objectius (clàusules 5.2 i 6.2)
- Metodologia d'avaluació i tractament de riscos (clàusula 6.1.2)
- Pla de tractament de risc (clàusula 6.1.3 e i 6.2)
- Informe sobre avaluació de riscos (clàusula 8.2)
- Definició de rols i responsabilitats de seguretat (clàusules A.7.1.2 i A.13.2.4)
- Inventari d'actius (clàusula A.8.1.1)
- Ús acceptable dels actius (clàusula A.8.1.3)
- Política de control d'accés (clàusula A.9.1.1)

• Procediments d'operació per a gestió de TI (clàusula A.12.1.1)
• Principis d'enginyeria de sistemes segurs (clàusula A.14.2.5)
• Política de seguretat per a proveïdors (clàusula A.15.1.1)
• Procediment per a gestió d'incidents (clàusula A.16.1.5)
• Procediments de Continuïtat de negoci (clàusula A.17.1.2)
• Requeriments legals, regulatoris i contractuals (clàusula A.18.1.1)
I aquí hi ha els registres obligatoris:
• Registres de formació, habilitats, experiència i qualificacions (clàusula 7.2)
• Seguiment i resultats de mesurament (clàusula 9.1)
• Programa d'auditoria interna (clàusula 9.2)
• Resultats d'auditories internes (clàusula 9.2)
• Resultats de la Revisió per Direcció (clàusula 9.3)
• Resultats d'accions correctives (clàusula 10.1)
• Registres de les activitats d'usuari, excepcions i esdeveniments de seguretat (clàusules A.12.4.1 i A.12.4.3)
• Procediment per a control de documents (clàusula 7.5)
• Controls per a la gestió de registres (clàusula 7.5)
• Política BYOD (Bring Your Own Device = Porta el propi dispositiu) (clàusula A.6.2.1)
• Política de dispositiu sobre dispositius mòbils i tele-treball (clàusula A.6.2.1)
• Política de classificació de la informació (clàusules A.8.2.1, A.8.2.2 i A.8.2.3)
• Política de claus (clàusules A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 i A.9.4.3)
• Política d'eliminació i destrucció (clàusules A.8.3.2 i A.11.2.7)
• Procediments per a treball en àrees segures (clàusula A.11.1.5)
• Política de pantalla i escriptori nets (clàusula A.11.2.9)
• Política de gestió de canvis (clàusules A.12.1.2 i A.14.2.4)
• Política de Còpies de seguretat (clàusula A.12.3.1)
• Política de transferència d'informació (clàusules A.13.2.1, A.13.2.2, i A.13.2.3)
• Anàlisi d'impacte en el negoci (BIA) (clàusula A.17.1.1)
• Pla de proves i verificació (clàusula A.17.1.3)
• Pla de manteniment i revisió (clàusula 17.1.3)
• Estratègia de continuïtat de negoci (clàusula A.17.2.1)

Annexa 8 Gestió d'indicadors

Nom indicador	Correu maliciós
Descripció	numero de d'obertures d'un correu "maliciós" prèviament dissenyat per incibe que obre una pàgina web amb indicacions del que els hi podria haver passat
Control de seguretat	formacions de conscienciació, educació i capacitació en SI
Formula de mesurament	A = nºPersones que obren el correu B = nº total Persones a les que s'envia correu X = A/B*100 = %
Unitats mesurament	%
Freqüència mesurament	3 mesos
Valor objectiu	0%
Valor de tall	Màxim 3%
Responsable de la mesura	Responsable de seguretat

Nom indicador	Access indegut
Descripció	numero de drets d'accés que no s'han retirat a personal que ja no treballa a la Fundació (mínim 5 dies des de la baixa)
Control de seguretat	9.2.6 Retirada o adaptació dels drets d'accés
Formula de mesurament	X = nº Persones que continuen tenint accés indegut
Unitats mesurament	Unitats
Freqüència mesurament	3 mesos
Valor objectiu	0
Valor de tall	2
Responsable de la mesura	Responsable de seguretat

Nom indicador	Revisió de politiques
Descripció	Revisió politiques de seguretat (comissió de seguretat)
Control de seguretat	5.1.2 Revisió de les polítiques per a la seguretat de la informació any
Formula de mesurament	Revisat o no revisat
Unitats mesurament	Si /no
Freqüència mesurament	Cada any
Valor objectiu	Si
Valor de tall	
Responsable de la mesura	Responsable de seguretat

Nom indicador	Teletreball
Descripció	Algun personal autoritzat pot realitzar teletreball mitjançant VPN Revisió instal·lacions teamvewer (mitjançant GLPI) Per que tothom utilitzi VPN
Control de seguretat	6.2.2 Teletreball
Formula de mesurament	Nº teamvwers instal.lats
Unitats mesurament	unitats
Freqüència mesurament	Trimestral
Valor objectiu	0
Valor de tall	0
Responsable de la mesura	Responsable de seguretat

Nom indicador	Contrasenyes savac
Descripció	Control contrasenyes segures His hospitalari Intentar descobrir les contrasenyes
Control de seguretat	Gestió de contrasenyes d'usuari.
Formula de mesurament	A = contrasenyes descobertes

	B = nº total contrasenyes X = A/B*100 = %
Unitats mesurament	%
Freqüència mesurament	6 mesos
Valor objectiu	0%
Valor de tall	5%
Responsable de la mesura	Responsable de seguretat

Nom indicador	**Entrada CPD 1**
Descripció	Registre entrades CPD1
Control de seguretat	11.1.2 Controls físics d'entrada. SI Control implantat per al CPD
Formula de mesurament	Nº intens entrada fraudulents
Unitats mesurament	unitats
Freqüència mesurament	3 mesos
Valor objectiu	0
Valor de tall	0
Responsable de la mesura	Responsable de seguretat

Nom indicador	**Temperatura CPD 2**
Descripció	Control de la temperatura al CPD2
Control de seguretat	11.1.4 Protecció contra les amenaces externes i ambientals
Formula de mesurament	T°> 34° durant mes de 5 minuts
Unitats mesurament	minuts
Freqüència mesurament	setmanal
Valor objectiu	5 minuts
Valor de tall	10 minuts
Responsable de la mesura	Responsable de seguretat

Nom indicador	Retirada dics durs
Descripció	Quan es retira un equip client s'ha de extreure el disc dur , etiquetar i guardar en un armari
Control de seguretat	11.2.7 Reutilització o retirada segura de dispositius d'emmagatzematge
Formula de mesurament	A=nº Disc retirats B=nº Pc retirats A/B = X
Unitats mesurament	Unitats
Freqüència mesurament	3 mesos
Valor objectiu	X=1
Valor de tall	X=1
Responsable de la mesura	Responsable de seguretat

Nom indicador	Documentar procediments
Descripció	Documentar els procediments operacionals
Control de seguretat	12.1.1 Documentació de procediments de operació.
Formula de mesurament	A=nº Documents B=nº Procediments A/B = X
Unitats mesurament	Unitats
Freqüència mesurament	6 mesos
Valor objectiu	X=1
Valor de tall	X<0.7
Responsable de la mesura	Responsable de seguretat

Nom indicador	Manteniment equips
Descripció	Espolsar equips amb compressor cada any al menys una vegada

Control de seguretat	11.2.4 Manteniment dels equips.
Formula de mesurament	A=nº equips espolsats B=nº equips clients A/B = X
Unitats mesurament	Unitats
Freqüència mesurament	1 any
Valor objectiu	X=1
Valor de tall	X< 0.7
Responsable de la mesura	Responsable de seguretat

Nom indicador	**Copies seguretat MV**
Descripció	Revisar copies seguretat (nivell politiques Nutanix) Nutanix fa copies segons política assignada a la MV
Control de seguretat	12.3.1 Còpies de seguretat de la informació.
Formula de mesurament	A=Copies correctes B= Copies incorrectes A/B=X
Unitats mesurament	unitats
Freqüència mesurament	6 mesos
Valor objectiu	X=1
Valor de tall	X< 0.8
Responsable de la mesura	Responsable de seguretat

Nom indicador	**Vulnerabilitats**
Descripció	Revisar actualitzacions dels programes mitjançant GLPI Gestionnaire Libre de Parc Informatique
Control de seguretat	12.6.1 Gestió de les vulnerabilitats tècniques
Formula de mesurament	A= software B= software desactualitzat A/B=X
Unitats mesurament	unitats
Freqüència mesurament	6 mesos

Valor objectiu	X=1
Valor de tall	X< 0.7
Responsable de la mesura	Responsable de seguretat

Nom indicador	**Restricció software**
Descripció	Revisar programes instal·lats mitjançant GLPI Gestionnaire Libre de Parc Informatique
Control de seguretat	14.2.4 Restriccions als canvis en els paquets de programari
Formula de mesurament	X=Numero Pc's amb sotfware no autoritzat
Unitats mesurament	unitats
Freqüència mesurament	6 mesos
Valor objectiu	X=0
Valor de tall	X< 2
Responsable de la mesura	Responsable de seguretat

Nom indicador	**SLA**
Descripció	Revisar contractes amb proveïdors externs, han d'haver signat SLA
Control de seguretat	15.1.2 Tractament del risc dins de acords de subministradors
Formula de mesurament	A=Numero contractes signats B= Numero proveïdors A/B=X
Unitats mesurament	unitats
Freqüència mesurament	1 any
Valor objectiu	X=1
Valor de tall	X=1
Responsable de la mesura	Responsable de seguretat

Nom indicador	Revisió esdeveniments seguretat
Descripció	Revisar fitxer de esdeveniments de seguretat, tots han de estar documentats correctament
Control de seguretat	16.1.2 Notificació dels esdeveniments de seguretat de la informació
Formula de mesurament	A=Numero esdeveniments B= Numero documentats correctament A/B=X
Unitats mesurament	unitats
Freqüència mesurament	1 any
Valor objectiu	X=1
Valor de tall	X=0.9
Responsable de la mesura	Responsable de seguretat

Nom indicador	Accés a dades
Descripció	Revisar acces a dades per part de personal no autoritzat ,
Control de seguretat	18.1.3 Protecció dels registres de la organització
Formula de mesurament	A=accessos no autoritzat a savac B= accessos no autoritzat a Aegerus (A+B) /2= X
Unitats mesurament	unitats
Freqüència mesurament	mensualment
Valor objectiu	X=0
Valor de tall	X=3
Responsable de la mesura	Responsable de seguretat

Nom indicador	Auditoria SGSI
Descripció	Auditoria externa es fa cada 2 anys
Control de seguretat	18.2.1 Revisió independent de la seguretat de la informació
Formula de mesurament	X= % no conformitats
Unitats mesurament	%
Freqüència mesurament	2 anys
Valor objectiu	X=0
Valor de tall	X=3%
Responsable de la mesura	Responsable de seguretat

Nom indicador	Recepta electrònica
Descripció	La recepta de medicaments es fa electrònicament, menys quant cau el servei que es fa amb paper
Control de seguretat	17.1.3 Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació
Formula de mesurament	X= % recepta en paper
Unitats mesurament	%
Freqüència mesurament	3 mesos
Valor objectiu	X=0%
Valor de tall	X=2%
Responsable de la mesura	Responsable de farmàcia /responsable de seguretat

Nom indicador	Intrusions virus
Descripció	Bitdefender registres activitat, Control de l'efectivitat de l'antivirus
Control de seguretat	12.2.1 Controls contra el codi maliciós.
Formula de mesurament	X= % virus no desinfectats , posats en cuarentena
Unitats mesurament	%
Freqüència mesurament	3 mesos

Valor objectiu	X=0%
Valor de tall	X=2%
Responsable de la mesura	Responsable de sistemes /seguretat

Nom indicador	**Altes usuari**
Descripció	Les altes s'han de fer mitjançant el GLPI (formulari alta)
Control de seguretat	9.2.1 Gestió d'altes / baixes en el registre de usuaris
Formula de mesurament	X= % usuaris donats d'alta GLPI
Unitats mesurament	%
Freqüència mesurament	6 mesos
Valor objectiu	X=0%
Valor de tall	X< 98%
Responsable de la mesura	Responsable de RRHH /responsable de seguretat

Annexa 9, Procediment de revisió de direcció

Aquest document té per objecte descriure les revisions que portarà a terme la alta direcció, sobre el sistema de gestió de la seguretat de la informació de la Fundació Hospital Sant Bernabé.

Aquestes revisions periòdiques han de permetre a la direcció tenir una visió de l'estat del SGSI, ja que son responsables de assignar i aportar recursos per que els sistemes d'informació funcionin amb garanties.

Procediment

La revisió de l'estat del SGSI es portarà a terme una vegada a l'any.

Aquestes revisions es registraran, en el registre hi haurà de constar:

- La data de la reunió
- Lloc de la reunió
- Hora de la reunió
- Assistents a la reunió

Es facilitarà a la direcció la següent informació :

- Resultats de les auditories i revisions anteriors
- Procediments que s'utilitzen en la organització i efectivitat del SGSI.
- Estat de les accions preventives i correctives
- Vulnerabilitats o amenaces no tractades en l'avaluació de riscos prèvia.
- Resultats dels indicadors dels controls.
- Accions de seguiment de les revisions gerencials prèvies.
- Canvis que afectin al SGSI.
- Recomanacions que hagin fet els empleats per millorar la seguretat.
- Formació sobre seguretat dels empleats.

Una vegada realitzada l'anàlisi, s'ha de obtenir:

• Modificacions que milloren l'efectivitat del SGSI.
• Actualització de la avaluació de riscos i el pla de tractament de riscos.
• Modificació de procediments i controls que afecten a la seguretat de la informació.
• Necessitats de recursos.
• Millora de com es valora l'efectivitat dels controls.

Planificació

Es planificaran les revisions de direcció per realitzar-les una vegada a l'any, després de l'auditoria interna .

Annexa 10 Gestió de Rols i Responsabilitats

L'objectiu d'aquest document es determinar els rols que intervenen en la seguretat i les funcions de cada un.

ORGANITZACIÓ DE LA SEGURETAT

La Política de Seguretat, segons requereix l'Annex II de l'ENS en la seva secció 3.1, ha d'identificar uns clars responsables per vetllar pel seu compliment i ser coneguda per tots els membres de l'organització administrativa.

S'estableixen els següents rols en l'organització relacionats amb la Seguretat de la Informació.

Responsable de la Informació

Aquestes funcions seran assumides per, la Gerència, en representació del Patronat de la Fundació, aquest entén la missió de la Fundació, determina els objectius que es proposa assolir i respon de que s'aconsegueixin.

Les seves funcions seran les següents:

- Té la responsabilitat última de l'ús que es faci d'una certa informació i, per tant, de la seva protecció.
- És el responsable últim de qualsevol error o negligència que porti a un incident de confidencialitat o d'integritat.
- Estableix els requisits de la informació en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.
- Determinarà els nivells de seguretat en cada dimensió dins el marc establert en l'Annex I de l'ENS.

Encara que l'aprovació formal dels nivells correspongui al responsable de la Informació, podrà demanar una proposta al responsable de la Seguretat i convé que escolti l'opinió del responsable del Sistema.

Responsable de la seguretat de la informació

Comitè de seguretat

Funcions i responsabilitats.

El Comitè de Seguretat de la Informació, és l'òrgan que coordina la Seguretat de la Informació a nivell de la Fundació i es el responsable de aquesta.

En sessió celebrada en data 11 de març de 2011 es va constituir la Comissió de Seguretat .

Actualment l'any 2019 esta constituït per:

- La Secretaria tècnica,
- La direcció de la Unitat d'atenció a l'usuari,
- El Cap del departament d'Informàtica,
- El Responsable de admissions,
- i per representants de les àrees afectades per l'ENS

Els membres del Comitè de Seguretat de la Informació, son nomenats per la Gerència de la Fundació.

Les funcions del comitè són les següents:-

- Desenvolupar i mantenir l'estratègia corporativa de protecció
- Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè sigui aprovada per la Direcció.
- Aprovar la normativa de seguretat de la informació.
- Promoure la millora contínua del Sistema de Gestió de la Seguretat de la Informació.
- Atendre les inquietuds de la Corporació i dels diferents departaments.
- Informar regularment l'estat de la seguretat de la informació a l'Alta Direcció.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
- Monitoritzar els principals riscos residuals assumits per l'Organització i recomanar possibles actuacions respecte d'ells.
- Monitoritzar l'acompliment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'ells.
- Coordinació les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.

- Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Analitzar els informes d'Auditoria .
- Aprovar plans de millora de la seguretat de la informació de l'Organització.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i / o entre diferents àrees de l'Organització, elevant aquells casos en què no tingui prou autoritat per decidir.
- Exigir el compliment de les condicions de seguretat a tots nivells quan el tractament el realitzi un tercer, mitjançant l'elaboració de compromisos legals amb els encarregats externs de tractament.

El Comitè de Seguretat de la Informació no és un comitè tècnic, ha de demanar regularment del personal tècnic propi o extern, la informació pertinent per prendre decisions.

El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els quals hagi de decidir o emetre una opinió.

Aquest assessorament es determinarà en cada cas, podent materialitzar de diferents formes i maneres:

- Grups de treball especialitzats interns, externs o mixtes.
- Assessoria externa.
- Assistència a cursos o un altre tipus d'entorns formatius o d'intercanvi d'experiències.

Responsables de departaments

Els responsables de departaments, entenen què fa cada departament, i com es coordinen entre si per assolir els objectius marcats per la Direcció.

Funcions associades en quant a la seguretat

- Té la potestat de determinar els nivells de seguretat dels serveis dins el marc establert en l'Annex I de l'ENS.
- Té la responsabilitat última de l'ús que es faci de determinats serveis i, per tant, de la seva protecció. -
- És el responsable últim de qualsevol error o negligència que porti a un incident de disponibilitat dels serveis que gestiona.
- Encara que l'aprovació formal dels nivells correspongui al Responsable del Servei, podrà demanar una proposta al comitè de Seguretat i convé que escolti l'opinió del responsable de Tecnologies.

Responsable de Sistemes i de les tecnologies de la Informació (CIO)

Serà exercit pel Cap del Departament d'Informàtica, CIO

Les seves funcions seran les següents:

- Coordinar les necessitats de Seguretat de la Informació en el marc de la resta de necessitats de Seguretat Corporativa.
- Mantindrà la seguretat de la informació i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb el que estableix la Política de Seguretat de l'Organització.
- Promourà la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.
- Realitzarà l'Anàlisi de Riscos
- Elaborarà la declaració de Aplicabilitat a partir de les mesures de seguretat requerides d'acord a l'Annex II de l'ENS i del resultat de l'Anàlisi de Riscos.
- Ha de informar al responsable de la informació i al comitè de seguretat del nivell de risc residual esperat, després implementar les opcions de tractament seleccionades en l'anàlisi de riscos i les mesures de seguretat requerides pel ENS.
- Coordinarà l'elaboració de la Documentació de Seguretat del Sistema.
- Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per a la seva aprovació per Direcció.
- Participarà en l'elaboració i aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de Seguretat de la Informació.
- Elaborarà i aprovar els Procediments Operatius de Seguretat de la Informació.
- Ha de facilitar periòdicament al Comitè de Seguretat un resum d'actuacions en matèria de seguretat, d'incidents relatius a seguretat de la informació i l'estat de la seguretat del sistema (en particular del nivell de risc residual a què està exposat el sistema).
- Ha d'elaborar, al costat del Administrador de Sistemes, Plans de Millora de la Seguretat, per la seva aprovació pel Comitè de Seguretat de la Informació.
- Validarà els Plans de Continuïtat de Sistemes que elabori el Administrador de Sistemes, i que ha d'aprovar el Comitè de Seguretat de la Informació i provats periòdicament pel Responsable de Sistemes.
- Aprovarà les directrius proposades pel Administrador de Sistemes per a considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis.

- En cas d'ocurrència d'incidents de seguretat de la informació analitzarà i proposarà salvaguardes que previnguin incidents similars en un futur.
- Planificarà la implantació de les salvaguardes en el sistema
- Podrà designar els Delegats que consideri necessaris.

Per mitjà de la designació de Delegats, es delegaran funcions.

La responsabilitat final seguirà recaient sobre el responsable de la Seguretat.

Els delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegui el responsable de sistemes i de les tecnologies de la informació, podent ser, per exemple, la seguretat de sistemes d'informació concrets o de sistemes d'informació horitzontals. Cada responsable de seguretat Delegat tindrà una dependència funcional directa del CIO, que és a qui reporten.

Administrador de Sistemes

El Cap del departament d'informàtica nomenarà formalment al administrador de sistemes , una única persona en l'organització.

Les seves funcions seran les següents:

- La implementació, gestió i manteniment de les mesures de seguretat aplicables als Sistemes d'Informació.
- La gestió, configuració i actualització, si escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat dels Sistemes d'Informació.
- Desenvolupar, operar i mantenir els Sistemes de Informació durant tot el seu cicle de vida, les seves especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i sistema de gestió dels Sistemes d'Informació establint els criteris d'ús i els serveis disponibles en el mateix.
- El Responsable dels Sistemes pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els Responsables de la Informació afectada, del Servei afectat i amb el responsable de la Seguretat abans de ser executada. -
- Monitoritzar l'estat de la seguretat dels Sistemes d'Informació i reportar periòdicament o davant incidents de seguretat rellevants al responsable de Seguretat de la Informació.
- Elaborar els Plans de Continuïtat dels Sistemes perquè siguin validats pel coordinats i aprovats pel Comitè de Seguretat de la Informació.

- Realitzar exercicis i proves periòdiques dels Plans de Continuïtat del Sistema per mantenir-los actualitzats i verificar que són efectius.
- Informar els responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa.

Derivades del comitè de seguretat

- Assegurar-se que les mesures específiques de seguretat s'integrin adequadament dins el marc general de seguretat.
- Assegurar que els controls de seguretat establerts són complerts estrictament.
- Assegurar que la traçabilitat, pistes d'auditoria i altres registres de seguretat requerits es troben habilitats i registrin amb la freqüència desitjada, d'acord amb la Política de Seguretat establerta per l'Organització
- En cas d'ocurrència d'incidents de seguretat de la informació:
- Dur a terme el registre i gestió dels incidents de seguretat en els Sistemes sota la seva responsabilitat.
- Executar el pla de seguretat aprovat.
- Aïllar el incident per evitar la propagació a elements aliens a la situació de risc.
- Prendre decisions a curt termini si la informació s'ha vist compromesa de cap forma que pugui tenir conseqüències greus (aquestes actuacions haurien d'estar procedim entades per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Assegurar la integritat dels elements crítics del sistema si s'ha vist afectada la disponibilitat dels mateixos.
- Mantenir i recuperar la informació emmagatzemada pel Sistema i els seus serveis associats.
- Investigar l'incident: Determinar la manera, els mitjans, els motius i l'origen de l'incident.

Responsable de Recursos Humans

Els responsable de recursos humans s'ajustaran al que estableix l'ENS en matèria de personal de manera anàloga al que estableixen els punts anteriors.

El responsable de personal implantarà les mesures de seguretat que els competeixin dins de les determinades pel Comitè de Seguretat de la Informació, i informaran aquest del seu grau d'implantació, eficàcia i incidents.

DPD, Delegat de protecció de dades

Segons El Reglament General de Protecció de Dades (UE) 2016/679 (RGPD) de la Unió Europea (article 37) i Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia dels Drets Digitals, (article 34) la nostra Fundació esta obligada a comptar amb un delegat de Protecció de Dades com a centres sanitaris legalment obligat al manteniment de les històries clíniques dels pacients.

El Delegat de protecció de dades supervisa internament, el compliment de les obligacions que imposa el RGPD.

El mateix Reglament exigeix que tal figura tingui garantit un funcionament independent.

El delegat de protecció de dades serà designat atenent les seves qualitats professionals i, en particular, als seus coneixements especialitzats del Dret i la pràctica en matèria de protecció de dades i la seva capacitat per exercir les funcions indicades en l'article 39.

El delegat de protecció de dades podrà formar part de la plantilla del responsable o de l'encarregat del tractament o exercir les seves funcions en el marc d'un contracte de serveis.

El responsable o l'encarregat del tractament publicaran les dades de contacte del

delegat de protecció de dades i els comunicaran a l'autoritat de control.

El delegat de protecció de dades té, entre d'altres, les funcions següents:

- Informar i assessorar el responsable o l'encarregat i els treballadors sobre les obligacions que imposa la normativa de protecció de dades.
- Supervisar que es compleix la normativa.
- Assessorar respecte de l'avaluació d'impacte relativa a la protecció de dades.
- Cooperar amb l'autoritat de control.
- Actuar com a punt de contacte per a qüestions relatives al tractament.

Encarregat de tractament

És aquella persona física o jurídica que tracta dades personal per compte de l'Entitat. La relació jurídica entre l'encarregat extern del tractament haurà de ser regulada mitjançant el corresponent contracte per escrit. A més l'Entitat, en la mesura que pugui, certificats de compliment de la normativa relativa a la protecció de dades.

Les seves obligacions són garantir el compliment de les mesures establertes en el Document de Seguretat, així com les derivades de la normativa aplicable, i respectar totes les condicions contractuals que el vinculin amb l'entitat. L'Entitat es reservarà la potestat de requerir un certificat als Encarregats de Tractament perquè demostrin el seu compliment en matèria de protecció de dades.

L'Entitat disposa d'un llistat actualitzat amb tots els Encarregats de Tractament on es relaciona:

- L'empresa responsable de l'Encarregat de Tractament
- L'activitat desenvolupada
- La vigència del contracte

Usuaris

Usuari és tot aquell personal de l'Entitat amb accés a dades de caràcter personal. Aquest accés pot ser directe, motivat per raons de feina, o indirecte, per circumstàncies eventuals o per compartir espais de treball.

Les seves obligacions són complir les mesures de seguretat determinades per als fitxers que facin servir i reportar qualsevol incidència o mancança que detectin al responsable del fitxer o responsable de seguretat.

Relació amb el document de seguretat i protecció de dades personals.

Per a la prestació dels serveis de la Fundació han de ser tractats dades de caràcter personal. El Document o documents de Seguretat de la Fundació detallaran els fitxers afectats i els responsables corresponents, així com les mesures adoptades en el marc del Reial Decret 1720/2007 i normativa complementària. Tots els sistemes d'informació s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollides en l'esmenta't document

Annexa 11, **Metodologia de Anàlisis de Riscos**

MAGERIT

L'Objecte d'aquest document es descriure la tècnica de avaluació del risc que s'utilitzarà anomenada MAGERIT utilitzada per realitzar l'anàlisi de risc

Introducció

Magerit és una metodologia d'anàlisi i gestió de riscos dels Sistemes d'Informació elaborada pel Consell Superior d'Administració Electrònica del govern espanyol per minimitzar els riscos de la implantació i ús de les Tecnologies de la Informació, enfocada a les administracions públiques.

Actualment està en la seva versió 3.

Magerit ofereix una aplicació per a l'anàlisi i gestió de riscos d'un Sistema d'Informació.

Planificació

Activitats

1 - Caracterització de els actius Aquesta activitat busca identificar els actius rellevants dins el sistema a analitzar, caracteritzant pel tipus d'actiu, identificant les relacions entre els diferents actius, determinant en quines dimensions de seguretat són importants i valorant aquesta importància. El resultat d'aquesta activitat és l'informe anomenat "model de valor". A més a inclou unes Sub-tasques: a. Tasca MAR.11: Identificació dels actius b. Tasca MAR.12: Dependències entre actius c. Tasca MAR.13: Valoració dels actius

2 - Caracterització de les amenaces Aquesta activitat busca identificar les amenaces rellevants sobre el sistema a analitzar, caracteritzant per les estimacions de ocurrència (probabilitat) i dany causat (degradació). El resultat d'aquesta activitat és l'informe denominat "mapa de riscos". A més a inclou unes Sub-tasques: a. Tasca MAR.21: Identificació de les amenaces Tasca b. MAR.22: Valoració de les amenaces.

3 - Caracterització de les salvaguardes Aquesta activitat busca identificar les salvaguardes desplegades en el sistema a analitzar, qualificant-les per la seva eficàcia enfront de les amenaces que pretenen mitigar. El resultat d'aquesta activitat es concreta en diversos informes: • Declaració d'aplicabilitat. • Avaluació de salvaguardes. • Insuficiències (o vulnerabilitats del sistema de protecció). Inclou les següents Sub-tasques: a. Tasca MAR.31: identificació de les salvaguardes pertinents. b. Tasca MAR.32: Valoració de les salvaguardes

4 - Estimació de l'estat de risc Aquesta activitat processa totes les dades recopilades en les activitats anteriors per: • Realitzar un informe de l'estat de risc: estimació d'impacte i risc. • Realitzar un informe d'insuficiències: deficiències o debilitats en el

sistema de salvaguardes Inclou les següents Sub-tasques: • Tasca MAR.41: Estimació de l'impacte. • Tasca MAR.42: Estimació del risc **5 - Caracterització de els actius** Aquesta activitat consta de tres sub-tasques: • MAR.11: Identificació dels actius • MAR.12: Dependències entre actiu • MAR.13: Valoració dels actius [

Objectius de Magerit

directes:

1.conscienciar els responsables de les organitzacions d'informació de l'existència de riscos i de la necessitat de gestionar-los

2.oferir un mètode sistemàtic per analitzar els riscos derivats de l'ús de tecnologies de la informació i comunicacions (TIC)

3.ajudar a descobrir i planificar el tractament oportú per mantenir els riscos sota control

indirectes:

4.preparar a l'Organització per a processos d'avaluació, auditoria, certificació o acredita-ció, segons correspongui en cada cas

També s'ha buscat la uniformitat dels informes que recullen les troballes i les conclusions-nes de les activitats d'anàlisi i gestió de riscos:

Model de valor

Caracterització del valor que representen els actius per a l'Organització així com de les dependències entre els diferents actius.

Mapa de riscos

Relació de les amenaces a què estan exposats els actius.

Declaració d'aplicabilitat

Per a un conjunt de salvaguardes, s'indica si són d'aplicació en el sistema de informa-ció sota estudi o si, per contra, no tenen sentit.

Avaluació de salvaguardes

Avaluació de l'eficàcia de les salvaguardes existents en relació al risc que afronten.

Estat de risc

Caracterització dels actius pel seu risc residual; és a dir, pel que pot passar

Informe d'insuficiències

Absència o debilitat de les salvaguardes que apareixen com oportunes per reduir els riscos sobre el sistema. És a dir, recull les vulnerabilitats del sistema, enteses com a punts feblement protegits pels quals les amenaces podrien materialitzar-se.

Compliment de normativa

Satisfacció d'uns requisits. Declaració que s'ajusta i és conforme a la normativa corresponent.

Pla de seguretat

Conjunt de projectes de seguretat que permeten materialitzar les decisions de tractament de riscos

ESTRUCTURA

La versió 3 de Magerit s'ha estructurat en dos llibres i una guia de tècniques:

Llibre I - Mètode -

Llibre II - Catàleg d'elements

Guia de Tècniques - Recull de tècniques de diferent tipus que poden ser d'utilitat pa-ra l'aplicació del mètode.

Tipus d'actius

Actius essencials
En un sistema d'informació hi ha 2 coses essencials: - la **informació** que es maneja i - els **serveis** que presten. Aquests actius essencials marquen els requisits de seguretat per a tots els altres components del sistema.

- Actius essencials
  - Dades de caràcter personal
- Arquitectura del sistema
- [D] Dades / Informació
- [K] Claus criptogràfiques
- [S] Serveis
- [SW] Programari - Aplicacions informàtiques
- [HW] Equipament informàtic (maquinari)
- [COM] Xarxes de comunicacions
- [Media] Suports d'informació
- [AUX] Equipament [L] Instal·lacions
- [P] Personal

Dimensions de valoració
[D] Disponibilitat
[I] Integritat de les dades
[C] Confidencialitat de la informació
[A] Autenticitat
[T] Traçabilitat

Criteris de valoració Escales estàndard

S'ha triat una escala detallada de 5 valors, deixant en valor 0 com a determinant del que seria un valor menyspreable (a efectes de risc).

[Pi] Informació de caràcter personal

5 probablement afecti greument a un grup d'individus /probablement trenqui seriosament lleis o regulacions
4 probablement trenqui lleis o regulacions / probablement afecti un grup d'individus
3 probablement afecti un individu /probablement suposi l'incompliment d'una llei o regulació
2 pogués causar molèsties a un individu / pogués trencar de forma lleu lleis o regulacions
1 pogués causar molèsties a un individu/ probablement trenqui seriosament la llei o algun reglament de protecció d'informació personal

[LPO] Obligacions legals
5 probablement causi un ***incompliment excepcionalment greu*** d'una llei o re regulació
4 probablement causi un ***incompliment greu*** d'una llei o regulació
3 probablement sigui causa ***d'incompliment lleu*** o tècnic d'una llei o regulació
1 pogués causar l'incompliment lleu o tècnic d'una llei o regulació

[Si] Seguretat
5 probablement sigui causa d'un incident excepcionalment seriós de seguretat o dificulti la investigació d'incidents excepcionalment seriosos
4 probablement sigui causa d'un seriós incident de seguretat o dificulti la investiga ció d'incidents seriosos
3. probablement sigui causa d'un greu incident de seguretat o dificulti la investiga ció d'incidents greus
2 probablement sigui causa d'una minva en la seguretat o dificulti la investigació ció d'un incident
1 pogués causar una minva en la seguretat o dificultar la investigació d'un inci dent

[Dóna] Interrupció del servei

5 Probablement causi una ***interrupció excepcionalment seriosa*** de les activitats pròpies de l'Organització amb un seriós impacte en altres organitzacions

4 Probablement tingui un ***seriós impacte*** en altres organitzacions

3 Probablement causi una interrupció seriosa de les activitats pròpies de l'Organització amb un **impacte significatiu** en altres organitzacions
2 Probablement tingui un gran impacte en altres organitzacions
1 Probablement causi la interrupció d'activitats pròpies de l'Organització amb certimpacte en altres organitzacions

Amenaces

[N] Desastres naturals
- [N.1] Foc
- [N.2] Danys per aigua
- [N. *] Desastres naturals

[I] D'origen industrial
- [I.1] Foc
- [I.2] Danys per aigua
- [I. *] Desastres industrials
- [I.3] Contaminació mecànica
- [I.4] Contaminació electromagnètica
- [I.5] Avaria d'origen físic o lògic
- [I.6] Tall del subministrament
- [I.7] Condicions inadequades de temperatura o humitat
- [I.8] Fallada de serveis de
- [I.9] Interrupció d'altres serveis i subministraments essencials
- [I.10] Degradació dels suports d'emmagatzematge de la informació
- [I.11] Emanacions electromagnètiques

[I] Errors i errors no intencionats
- [E.1] Errors dels usuaris
- [E.2] Errors del administrador
- [E.3] Errors de monitoratge (log)
- [E.4] Errors de configuració
- [E.7] Deficiències en l'organització
- [E.8] Difusió de programari perjudicial
- [E.9] Errors de [re-] encaminament
- [E.10] Errors de seqüència
- [E.14] Fuites d'informació
- [E.15] Alteració accidental de la informació
- [E.18] Destrucció d'informació
- [E.19] Fuites d'informació
- [E.20] Vulnerabilitats dels programes (programari)
- [E.21] Errors de manteniment / actualització de programes (programari)
- [E.23] Errors de manteniment / actualització d'equips (maquinari)
- [I.24] Caiguda del sistema per esgotament de
- [I.25] Pèrdua d'equips
- [E.28] Indisponibilitat del personal

[A] Atacs intencionats

[A.3] Manipulació dels registres d'activitat (log)
[A.4] Manipulació de la configuració
[A.5] Suplantació de la identitat de l'usuari
[A.6] Abús de privilegis d'accés
[A.7] Ús no previst
[A.8] Difusió de programari perjudicial
[A.9] [Re-] encaminament de missatges
[A.10] Alteració de seqüència
[A.11] Accés no autoritzat
[A.12] Anàlisi de trànsit
[A.13] Repudi
[A.14] Intercepció d'informació (escolta)
[A.15] Modificació deliberada de la informació
[A.18] Destrucció d'informació
[A.19] Divulgació d'informació
[A.22] Manipulació de programes
[A.23] Manipulació dels equips
[A.24] Denegació de servei
[A.25] Robatori
[A.26] Atac destructiu
[A.27] Ocupació enemiga
[A.28] Indisponibilitat del personal
[A.29] Extorsió
[A.30] Enginyeria social (picaresca)

Salvaguardes

Proteccions generals o horitzontals
Protecció de les dades / informació
Protecció de les claus criptogràfiques
Protecció dels serveis
Protecció de les aplicacions (programari)
Protecció dels equips (maquinari)
Protecció de les comunicacions
Protecció en els punts d'interconnexió amb altres sistemes
Protecció dels suports d'informació
Protecció dels elements auxiliars
Seguretat física - Protecció de les instal·lacions
Salvaguardes relatives al personal
Salvaguardes de tipus organitzatiu
Continuïtat d'operacions
Externalització
Adquisició i desenvolupament

Procediment

1-identificació dels actius, amb un codi i un nom descriptiu
2- identificació de quin tipus (s) cal classificar l'actiu
3- identificació de les dependències entre actius
4- valoració dels actius en diferents dimensions

Informes

A4.1. Model de valor Caracterització del valor que representen els actius per a l'Organització així com de les dependències entre els diferents actius

1. Identificació del projecte Codi, descripció, propietari, organització. Versió, data. Biblioteca de referència.
2. Actius
    2.1. Arbre d'actius (relacions de dependència)
    2.2. Valoració dels actius (valor propi) Indicant la raó de la valoració atribuïda a cada actiu en cada dimensió.

A4.2. Mapa de riscos Relació de les amenaces a què estan exposats els actius

1. Identificació del projecte Codi, descripció, propietari, organització. Versió, data. Biblioteca de referència.
2. Actius
    2.1. Arbre d'actius (relacions de dependència)
    2.2. Valoració dels actius (valor propi) Indicant la raó de la valoració atribuïda a cada actiu en cada dimensió.
3. Amenaces per actiu Per a cada actiu:
    - amenaces rellevants
    - degradació estimada en cada dimensió
    - freqüència anual estimada
4. Actius per amenaça
Per a cada amenaça:
    - actius afectats
    - degradació estimada en cada dimensió
    - freqüència anual estimada

A4.3. Avaluació de salvaguardes Avaluació de l'eficàcia de les salvaguardes existents en relació al risc que afronten.

1. Identificació del projecte Codi, descripció, propietari, organització. Versió, data. Biblioteca de referència.
2. Salvaguardes

Per a cada salvaguarda, al nivell de detall que s'estimi oportú, indicació de la seva eficàcia davant els riscos als quals s'enfronta.
Si escau, mostrar l'evolució històrica i la planificació actual.

A4.4. Estat de risc Caracterització dels actius pel seu risc residual; és a dir el que pot passar tenint en compte les salvaguardes desplegades

1. Identificació del projecte Codi, descripció, propietari, organització. Versió, data. Biblioteca de referència.
2. Actius Per a cada actiu:
    1. Impacte acumulat
    2. Risc acumulat
    3. Impacte repercutit
    4. Risc repercutit Si escau, mostri l'evolució històrica i l'efecte de la planificació actual.

A4.5. Informe d'insuficiències Absència o debilitat de les salvaguardes que apareixen com oportunes per reduir el risc sobre el sistema.
1. Identificació del projecte Codi, descripció, propietari, organització. Versió, data. Biblioteca de referència.
2. Salvaguardes
Per a cada salvaguarda, al nivell de detall que s'estimi oportú, l'eficàcia sigui inferior a un llindar determinat, indicació de la seva eficàcia davant els riscos als quals es en s'enfronta. Si escau, mostri l'evolució històrica i la planificació actual.

A4.6. Pla de seguretat Conjunt de programes de seguretat que permeten materialitzar les decisions de gestió de riscos.

1. Marc de referència
    - Política de seguretat de l'organització
    - Relació de normes i procediments
2. Responsables i responsabilitats (a nivell d'organització)
3. Programes de seguretat Per cada programa identificat:
    - objectiu genèric
    - prioritat o urgència
    - ubicació temporal: quan es durà a terme?
    - salvaguardes involucrades
    - unitat responsable de la seva execució
    - estimació de costos financers
    - estimació de recursos
    - estimació d'impacte per a l'organització

    Quan arriba el moment per ser escomès, cada programa de seguretat ha de detallar: • El seu objectiu genèric.

• Les salvaguardes concretes a implantar o millorar, detallant els seus objectius de qualitat, eficiència eficàcia i eficiència
• La relació d'escenaris d'impacte i / o risc que afronta: actius afectats, tipus d'acti vós, amenaces afrontades, valoració d'actius i amenaces i nivells d'impacte i risc
• La unitat responsable de la seva execució.
• Una estimació de costos, tant econòmics com d'esforç de realització, tenint en compte: • costos d'adquisició (de productes), o de contractació (de serveis), o de desenvolupament (de solucions clau en mà), podent ser necessari avaluar diferents alternatives
• costos d'implantació inicial i manteniment en el temps
• costos de formació, tant dels operadors com dels usuaris, segons convingui al cas
• costos d'explotació
• impacte en la productivitat de l'Organització
• Una relació de subtasques a afrontar, tenint en compte
• canvis en la normativa i desenvolupament de procediments
• solució tècnica: programes, equips, comunicacions i locals,
• pla de desplegament
• pla de formacio
•Una estimació del temps d'execució des de la seva arrencada fins a la seva posada en operació.
• Una estimació de l'estat de risc (impacte i risc residual al seu compleció).
• Un sistema d'indicadors d'eficàcia i eficiència que permetin conèixer en cada moment la qualitat de l'acompliment de la funció de seguretat que es desitja i la seva evolució temporal

TECNIQUES

Impacte i risc

Sigui l'escala següent útil per qualificar el valor dels actius, la magnitud de l'impacte i la magnitud del risc:
• **MB:** molt baix
• **B:** sota
• **M:** mitjà
• **A:** alt
• **MA:** molt alt

Estimació de l'impacte Es pot calcular l'impacte sobre la base de taules senzilles de doble entrada:

impacte		degradació		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Estimació del risc D'altra banda es modelen impacte, probabilitat i risc per mitjà d'escales qualitatives:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Podent combinar impacte i freqüència en una taula per calcular el risc:

risc		probabilidad				
		MB	B	M	A	MA
impacte	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Annexa 12 Aplicabilitat dels controls

	Aplica
5. POLÍTIQUES DE SEGURETAT.	
5.1 Directrius de la Direcció en seguretat de la informació.	
5.1.1 Conjunt de polítiques per a la seguretat de la informació.	Si
5.1.2 Revisió de les polítiques per a la seguretat de la informació.	Si
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	
6.1 Organització interna.	
6.1.1 Assignació de responsabilitats per a la segur. de la informació.	Si
6.1.2 Segregació de tasques.	Si
6.1.3 Contacte amb les autoritats.	Si
6.1.4 Contacte amb grups d'interès especial.	Si
6.1.5 Seguretat de la informació en la gestió de projectes.	Si
6.2 Dispositius per a mobilitat i teletreball.	
6.2.1 Política d'ús de dispositius per mobilitat.	Si
6.2.2 Teletreball.	Si
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS.	
7.1 Abans de la contractació.	
7.1.1 Investigació d'antecedents.	Si
7.1.2 Condicions de contractació.	Si
7.2 Durant la contractació.	
7.2.1 Responsabilitats de gestió.	Si
7.2.2 Conscienciació, educació i capacitació en segur. de la informació	Si
7.2.3 Procés disciplinari.	Si
7.3 Cessament o canvi de lloc de treball.	
7.3.1 Cessament o canvi de lloc de treball.	Si
8. GESTIÓ D'ACTIUS.	
8.1 Responsabilitat sobre els actius.	
8.1.1 Inventari d'actius.	Si

8.1.2 Propietat dels actius.	Si
8.1.3 Ús acceptable dels actius.	Si
8.1.4 Devolució d'actius.	Si
8.2 Classificació de la informació.	
8.2.1 Directrius de classificació.	Si
8.2.2 Etiquetatge i manipulat de la informació.	Si
8.2.3 Manipulació d'actius.	Si
8.3 Maneig dels suports d'emmagatzematge.	
8.3.1 Gestió de suports extraïbles.	Si
8.3.2 Eliminació de suports.	Si
8.3.3 Suports físics en trànsit.	Si
9. CONTROL D'ACCESSOS.	
9.1 Requisits de negoci per al control d'accessos.	
9.1.1 Política de control d'accessos.	Si
9.1.2 Control d'accés a les xarxes i serveis associats.	Si
9.2 Gestió d'accés d'usuari.	
9.2.1 Gestió d'altes / baixes en el registre de usuaris.	Si
9.2.2 Gestió dels drets d'accés assignats a usuaris.	Si
9.2.3 Gestió dels drets d'accés amb privilegis especials.	Si
9.2.4 Gestió d'informació confidencial de autenticació d'usuaris.	Si
9.2.5 Revisió dels drets d'accés de els usuaris.	Si
9.2.6 Retirada o adaptació dels drets d'accés	Si
9.3 Responsabilitats de l'usuari.	
9.3.1 Ús d'informació confidencial per a la autenticació.	Si
9.4 Control d'accés a sistemes i aplicacions.	
9.4.1 Restricció de l'accés a la informació. SI Existeix un control d'accessos selectiu.	Si
9.4.2 Procediments segurs d'inici de sessió.	Si
9.4.3 Gestió de contrasenyes d'usuari.	si
9.4.4 Ús d'eines d'administració de sistemes.	Si
9.4.5 Control d'accés al codi font dels programes.	Si
10. XIFRAT.	

10.1 Controls criptogràfics.	
10.1.1 Política d'ús dels controls criptogràfics.	Si
10.1.2 Gestió de claus. SI Existeixen claus de xifratge dels Equips d'oficines.	Si
11. SEGURETAT FÍSICA I AMBIENTAL.	
11.1 Àrees segures.	
11.1.1 perímetre de seguretat física. SI Control implantat per al CPD. (Ja implementat)	Si
11.1.2 Controls físics d'entrada. SI Control implantat per al CPD. (Ja implementat)	Si
11.1.3 Seguretat d'oficines, despatxos i recursos.	Si
11.1.4 Protecció contra les amenaces externes i ambientals.	Si
11.1.5 El treball en àrees segures. SI Control implantat per al CPD. (Ja implementat)	Si
11.1.6 Àrees d'accés públic, càrrega i descàrrega.	Si
11.2 Seguretat dels equips.	
11.2.1 Emplaçament i protecció d'equips. SI Existeixen Equips sensibles.	Si
11.2.2 Instal·lacions de subministrament. SI Control implantat per al CPD. (Ja implementat)	Si
11.2.3 Seguretat del cablejat. SI Control implantat per al CPD. (Ja implementat)	Si
11.2.4 Manteniment dels equips. SI És realitza Manteniment dels equips.	Si
11.2.5 Sortida d'actius fora de les dependències de l'empresa.	Si
11.2.6 Seguretat dels equips i actius fora de les instal·lacions.	Si
11.2.7 Reutilització o retirada segura de dispositius d'emmagatzematge.	Si
11.2.8 Equip informàtic d'usuari desatès.	Si
11.2.9 Política de lloc de treball buidat i bloqueig de pantalla.	Si
12. SEGURETAT A L'OPERATIVA.	
12.1 Responsabilitats i procediments d'operació.	
12.1.1 Documentació de procediments de operació.	Si
12.1.2 Gestió de canvis.	Si
12.1.3 Gestió de capacitats.	Si
12.1.4 Separació d'entorns de desenvolupament, prova i producció.	Si
12.2 Protecció contra codi maliciós.	
12.2.1 Controls contra el codi maliciós.	Si

12.3 Còpies de seguretat.	
12.3.1 Còpies de seguretat de la informació.	Si
12.4 Registre d'activitat i supervisió.	
12.4.1 Registre i gestió d'esdeveniments de activitat.	Si
12.4.2 Protecció dels registres d'informació.	Si
12.4.3 Registres d'activitat de l'administrador i operador del sistema.	Si
12.4.4 Sincronització de rellotges.	Si
12.5 Control del programari en explotació.	
12.5.1 Instal·lació del programari en sistemes en producció.	Si
12.6 Gestió de la vulnerabilitat tècnica.	
12.6.1 Gestió de les vulnerabilitats tècniques.	Si
12.6.2 Restriccions en la instal·lació de programari.	Si
12.7 Consideracions de les auditories dels sistemes d'informació.	
12.7.1 Controls d'auditoria dels sistemes de informació.	Si
13. SEGURETAT A LES TELECOMUNICACIONS.	
13.1 Gestió de la seguretat en les xarxes.	
13.1.1 Controls de xarxa.	Si
13.1.2 Mecanismes de seguretat associats a serveis en xarxa.	Si
13.1.3 Segregació de xarxes.	Si
13.2 Intercanvi d'informació amb parts externes.	
13.2.1 Polítiques i procediments d'intercanvi d'informació.	Si
13.2.2 Acords d'intercanvi.	Si
13.2.3 Missatgeria electrònica.	Si
13.2.4 Acords de confidencialitat i secret.	Si
14. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ.	
14.1 Requisits de seguretat dels sistemes d'informació.	
14.1.1 Anàlisi i especificació dels requisits de seguretat.	Si
14.1.2 Seguretat de les comunicacions en serveis accessibles per xarxes públiques.	Si
14.1.3 Protecció de les transaccions per xarxes telemàtiques.	Si
14.2 Seguretat en els processos de desenvolupament i suport.	
14.2.1 Política de desenvolupament segur de programari. NO L'organització no	Si

desenvolupa programari.	
14.2.2 Procediments de control de canvis en els sistemes.	Si
14.2.3 Revisió tècnica de les aplicacions després efectuar canvis en el sistema operatiu.	Si
14.2.4 Restriccions als canvis en els paquets de programari.	Si
14.2.5 Ús de principis d'enginyeria en protecció de sistemes.	Si
14.2.6 Seguretat en entorns de desenvolupament.	Si
14.2.7 Externalització del desenvolupament de programari	Si
14.2.8 Proves de funcionalitat durant el desenvolupament dels sistemes.	Si
14.2.9 Proves d'acceptació.	Si
14.3 Dades de prova.	
14.3.1 Protecció de les dades utilitzades en proves.	Si
15. RELACIONS AMB SUBMINISTRADORES.	
15.1 Seguretat de la informació en les relacions amb subministradors.	
15.1.1 Política de seguretat de la informació per subministradors.	Si
15.1.2 Tractament del risc dins de acords de subministradors.	Si
15.1.3 Cadena de subministrament en tecnologies de la informació i comunicacions.	Si
15.2 Gestió de la prestació del servei per subministradors.	
15.2.1 Supervisió i revisió dels serveis prestats per tercers.	Si
15.2.2 Gestió de canvis en els serveis prestats per tercers.	Si
16. GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	Si
16.1 Gestió d'incidents de seguretat de la informació i millores.	
16.1.1 Responsabilitats i procediments.	Si
16.1.2 Notificació dels esdeveniments de seguretat de la informació.	Si
16.1.3 Notificació de punts febles de la seguretat.	Si
16.1.4 Valoració d'esdeveniments de seguretat de la informació i presa de decisions.	Si
16.1.5 Resposta als incidents de seguretat.	Si
16.1.6 Aprenentatge dels incidents de seguretat de la informació.	Si
16.1.7 Recull d'evidències.	Si
17. SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.	
17.1 Continuïtat de la seguretat de la informació.	

17.1.1 Planificació de la continuïtat de la seguretat de la informació.	Si
17.1.2 Implantació de la continuïtat de la seguretat de la informació.	Si
17.1.3 Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	Si
17.2 Redundàncies.	
17.2.1 Disponibilitat d'instal·lacions per al processament de la informació.	Si
18. COMPLIMENT.	
18.1 Compliment dels requisits legals i contractuals.	
18.1.1 Identificació de la legislació aplicable.	Si
18.1.2 Drets de propietat intel·lectual (DPI).	Si
18.1.3 Protecció dels registres de la organització.	Si
18.1.4 Protecció de dades i privacitat de la informació personal.	Si
18.1.5 Regulació dels controls criptogràfics.	Si
18.2 Revisions de la seguretat de la informació.	
18.2.1 Revisió independent de la seguretat de la informació.	Si
18.2.2 Compliment de les polítiques i normes de seguretat.	Si

Annexa 13: Anàlisis de risc, resum executiu

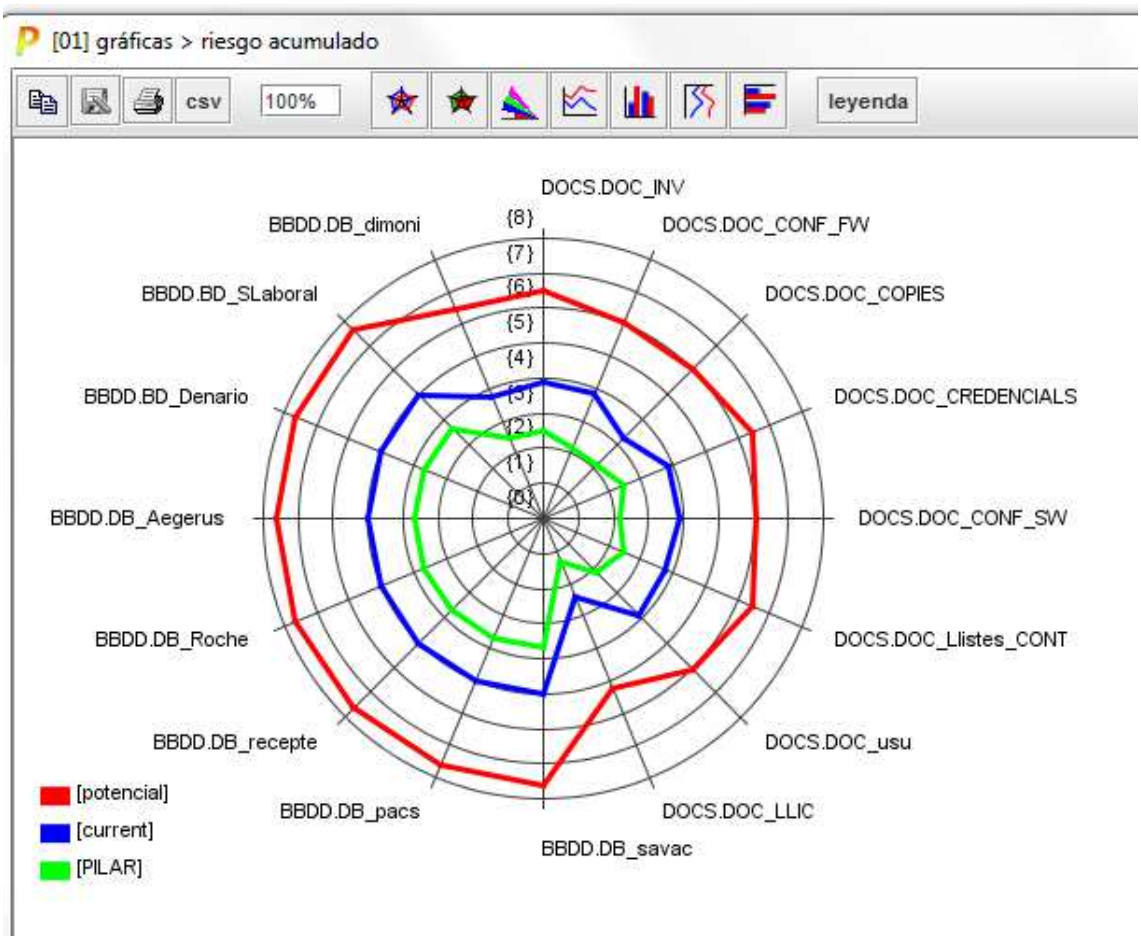
** es pot obrir fitxer "tfm" per revisar la informació*

En aquesta fase he analitzat l'informe d'insuficiències i l'anàlisi de risc obtingut, juntament amb l'avaluació de les salvaguardes.

Faig un resum de les conclusions de l'anàlisi

4. Domini de seguretat : Base

4.1 [D] Protecció de la Informació



Fase 2.4 /pàgina 1

Falta un gestor documental per registrar, etiquetar, classificar la informació, actualment es troba:

Documents d'usuaris

en carpetes accessibles nomes pel seu autor en el servidor, s'accedeix amb usuari de active directory i es fan copies de seguretat.

Informes assistencials

En les bases de dades de Savac

Intranet

informació pel personal

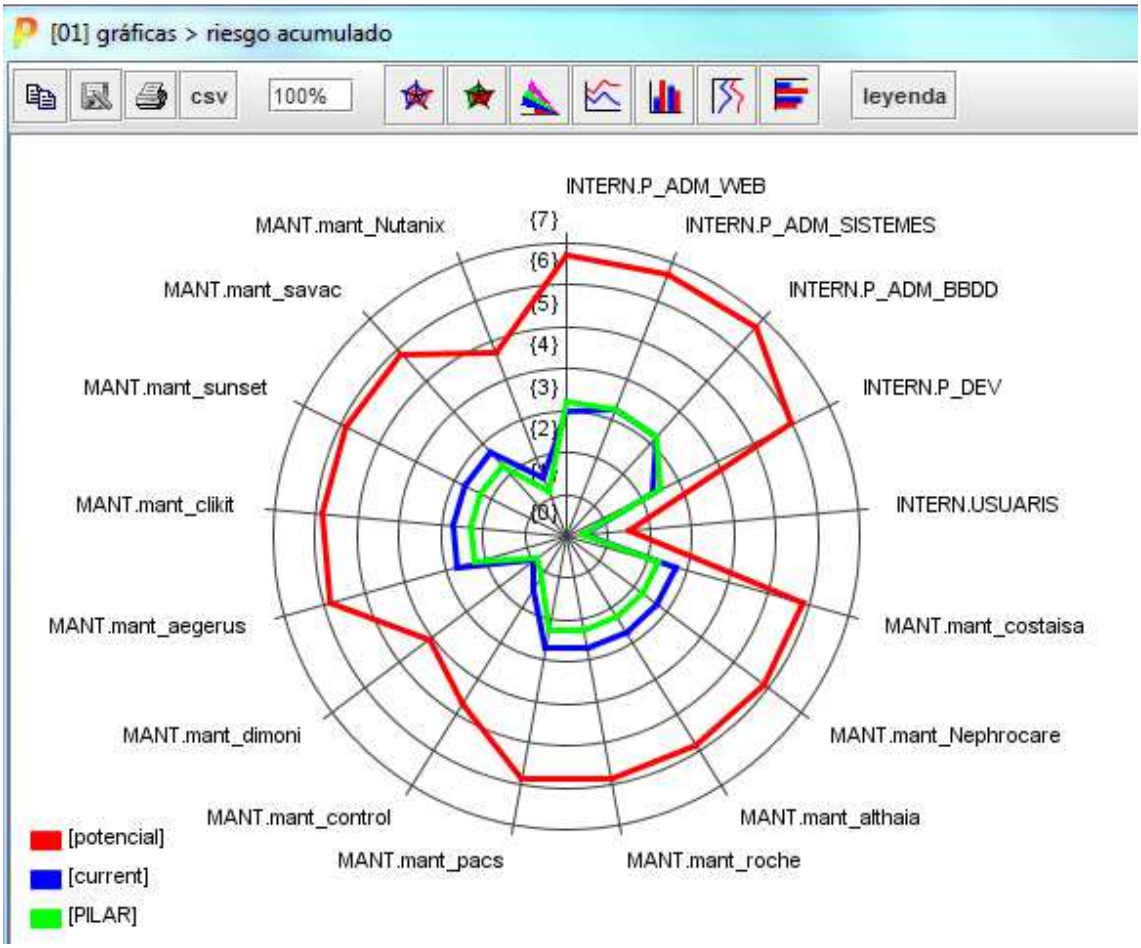
Projectes detectats punt 4.1

[PR01.41]Projecte gestió documentació i expedients

[PR02.41]Projecte redacció normativa per utilitzar gestor documental i arxivar els arxius (etiquetatge, nivell seguretat, versions, informació autor, etc..)

[PR03.41]Redacció de un estàndard de metodologia de copies de seguretat i un control de les mateixes

4.2[IA] IDENTIFICACIÓ I AUTENTICACIÓ



Cal normativa de altes baixes i modificacions d'usuaris, es un procés que es fa sempre igual però no esta descrit (L2) i formació a recursos humans, en aquest moment al fer un nou contracte des de recursos humans es demana l'usuari al departament de sistemes però no es fa el mateix quant el treballador deixa l'empresa.

Cal insistir en la necessitat de control de les baixes d'usuaris i no, nomes de les altes.

Cal automatitzar el canal de comunicació.

Projectes detectats punt 4.2

[PR01.42]Projecte automatització de peticions per gestionar usuaris

[PR02.42]Projecte redacció i difusió estàndard, gestió altes baixes i modificacions d'usuaris i privilegis d'aquests.

4.3[AC] CONTROL D'ACCÉS LÒGIC

L'accés als ordinadors clients es fa a traves d'un usuari i contrasenya que es gestiona en un active directory

Esta separat el rol que permet administrar el ordinador del de usuari.

Cada usuari dintre del directory te uns grups assignats (que a la vegada tenen politiques associades)

L'accés a les aplicacions amb dades confidencials , tenen integrat aquest directory o cal un altre usuari i contrasenya per accedir-hi

	Integració
Savac	No
Denario (portal del treballador)	No
Aegerus	No
Intranet	Si
Correu corporatiu	No
Dimoni	No
GLPI	Si

Dintre de Savac i Aegerus existeixen rols de accés a dades segons categoria

Projectes detectats punt 4.3

[PR01.43]Caldria integrar l'accés a les aplicacions mes important al directory actiu per simplificar la gestió dels usuaris.

4.4[PS] GESTIÓ DEL PERSONAL I ELS LLOCS DE TREBALL

Llocs de treball, tenim maquinari de reserva pels llocs mes habituals per si cal canviar un ordinador o una impressora en poc temps, restituint el lloc

Alguns ordinadors tenen una configuració especial per que estan connectats a aparells mèdics (ergonometre, laparoscòpia, espirometries ....) , d'aquest es fa una imatge i es guarda en un disc dur extern

El personal de sistemes es molt especialitzat en àrees concretes.

Cal documentar el coneixement del personal de sistemes en les seves àrees concretes i sobretot en les gestions o processos mes habituals.

Cal formar els membres de l'equip de sistemes en les gestions o processos mes habituals que no els hi pertoquen per poder-se substituir entre ells en les tasques bàsiques.

En quant als altres llocs de treball existeix una wiki que gestiona sistemes on es troba la documentació de les tasques que han de realitzar comunament en el HIS, Savac

- metges (Consulta externa, Hospitalització, Urgències, Quiròfan)
- infermeres (Planta, Urgències, Consulta externa)
- admissions

S'han de millorar els processos de gestió del coneixement pel personal de suplències o el de nova incorporació.

Projectes detectats punt 4.4

[PR01.44]Caldria copiar les configuracions de llocs de treball especials a la cabina de copies i crear una tasca de revisió de aquestes imatges cada 3 mesos o cada vegada que hi hagi un canvi.

[PR02.44]Caldria crear una wiki pels treballadors/es que utilitzen Aegerus a la residencia i afegir a la wiki del hospital les tasques de facturació, secretaria mèdica, comptabilitat, recursos humans.

Aquestes wikis s'haurien de revisar cada 6 mesos o cada vegada que hi hagin canvis.

4.5[TOOLS] EINES DE SEGURETAT

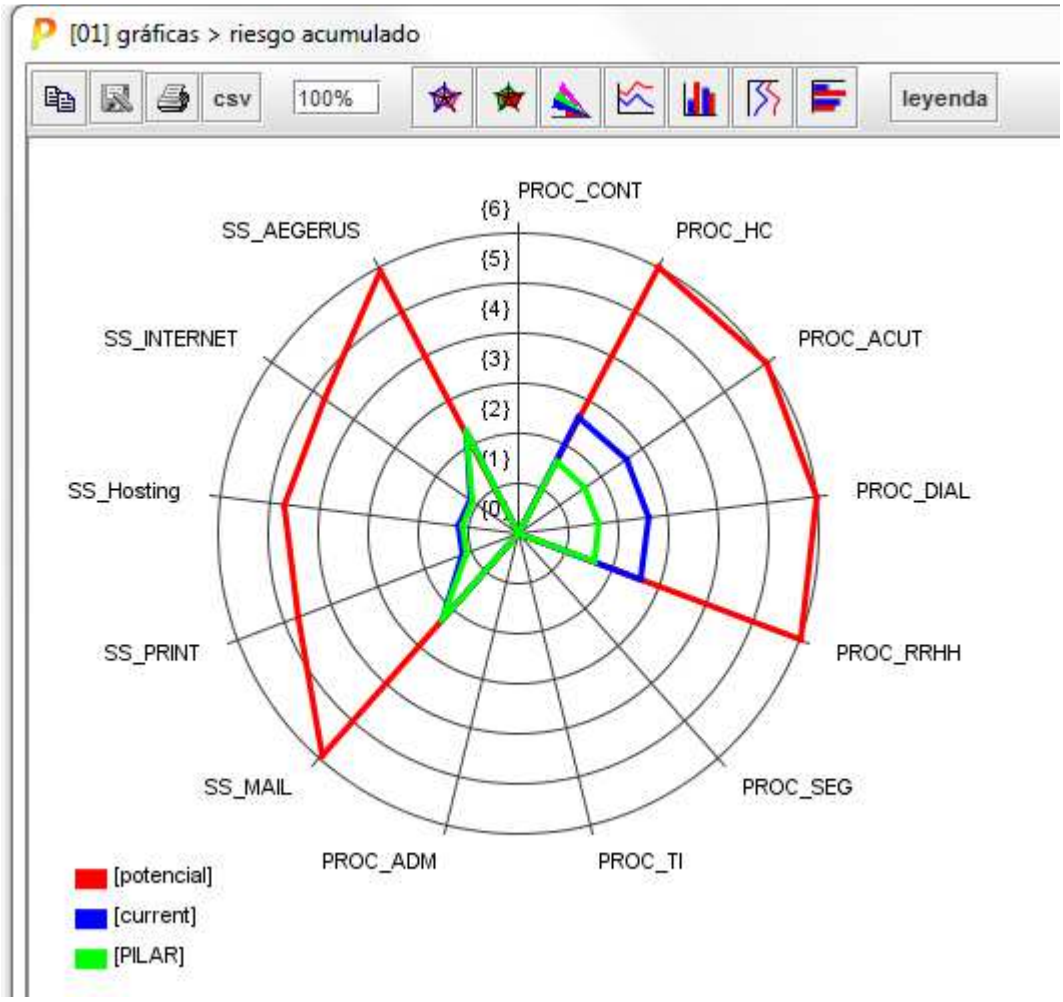
La fundació utilitza Bitdefender gestionat i centralitzat en un servidor com eina antivirus, tenim també 3 firewalls de nova generació , 2 en clúster a l'hospital i un a la residencia .

Es disposa d'un servidor que gestiona centralitzadament les actualitzacions de Windows

Projectes detectats punt 4.5

[PR01.45]Caldria automatitzar i descriure el processos de control tan en l'antivirus com en els firewalls.

4.6[S] PROTECCIÓ DELS SERVEIS



Cal millorar el procés S.3.7 Desmantellament de serveis que ja no s'utilitzen, sobretot desactivar el personal autoritzat (intern i extern) , podrien haver-hi VPN creades i rols de Windows i /o Savac , denario, aegerus...

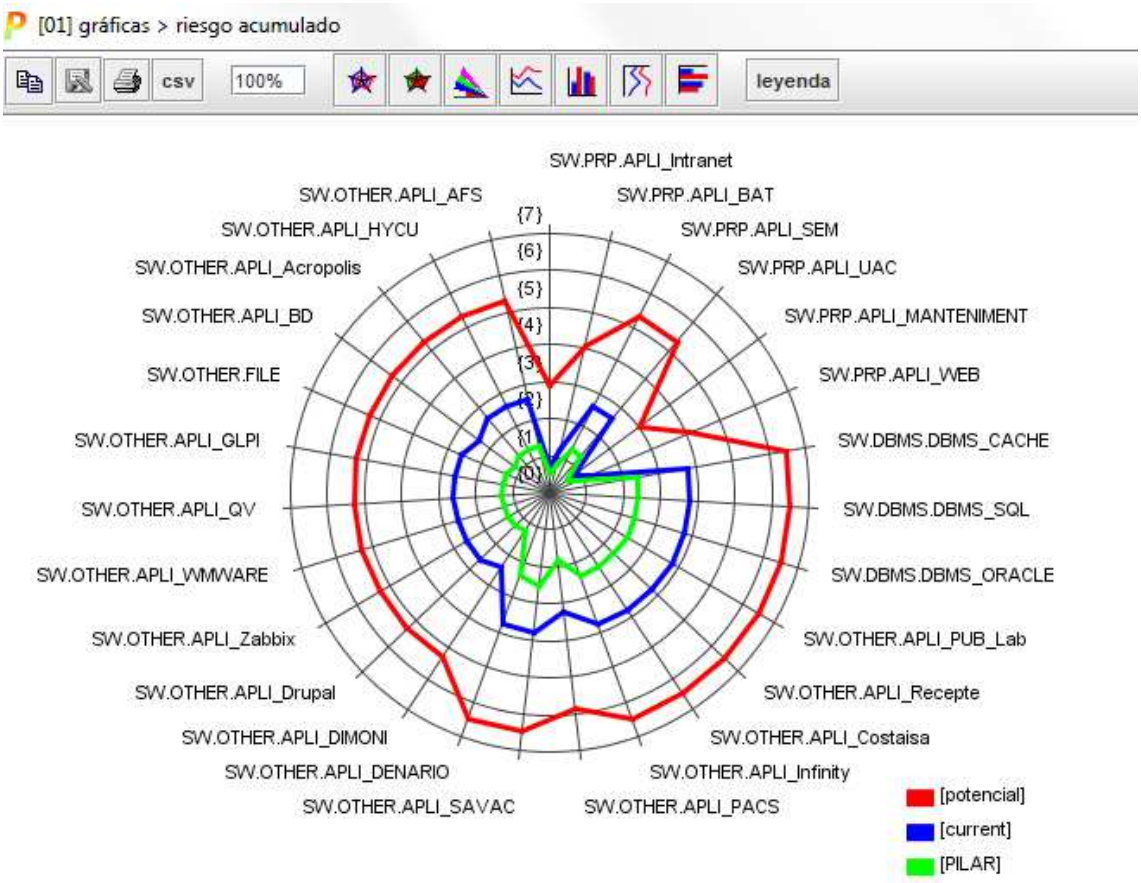
Aquet punt s'integra en l'apartat 4.2[IA] , on ja s'ha parlat de eliminar els usuaris que ja no treballen a la institució , aquí parlem d'eliminar els permisos als que ja no utilitzen un servei determinat.

També s'han de gestionar els canvis , inclou actualitzar procediments de producció i recuperació.

Projectes detectats punt 4.6

[PR01.46]Automatitzar i protocol·litzar els canvis de permisos i d'usuaris

4.7[SW] PROTECCIÓ DE LES APLICACIONS INFORMÀTIQUES



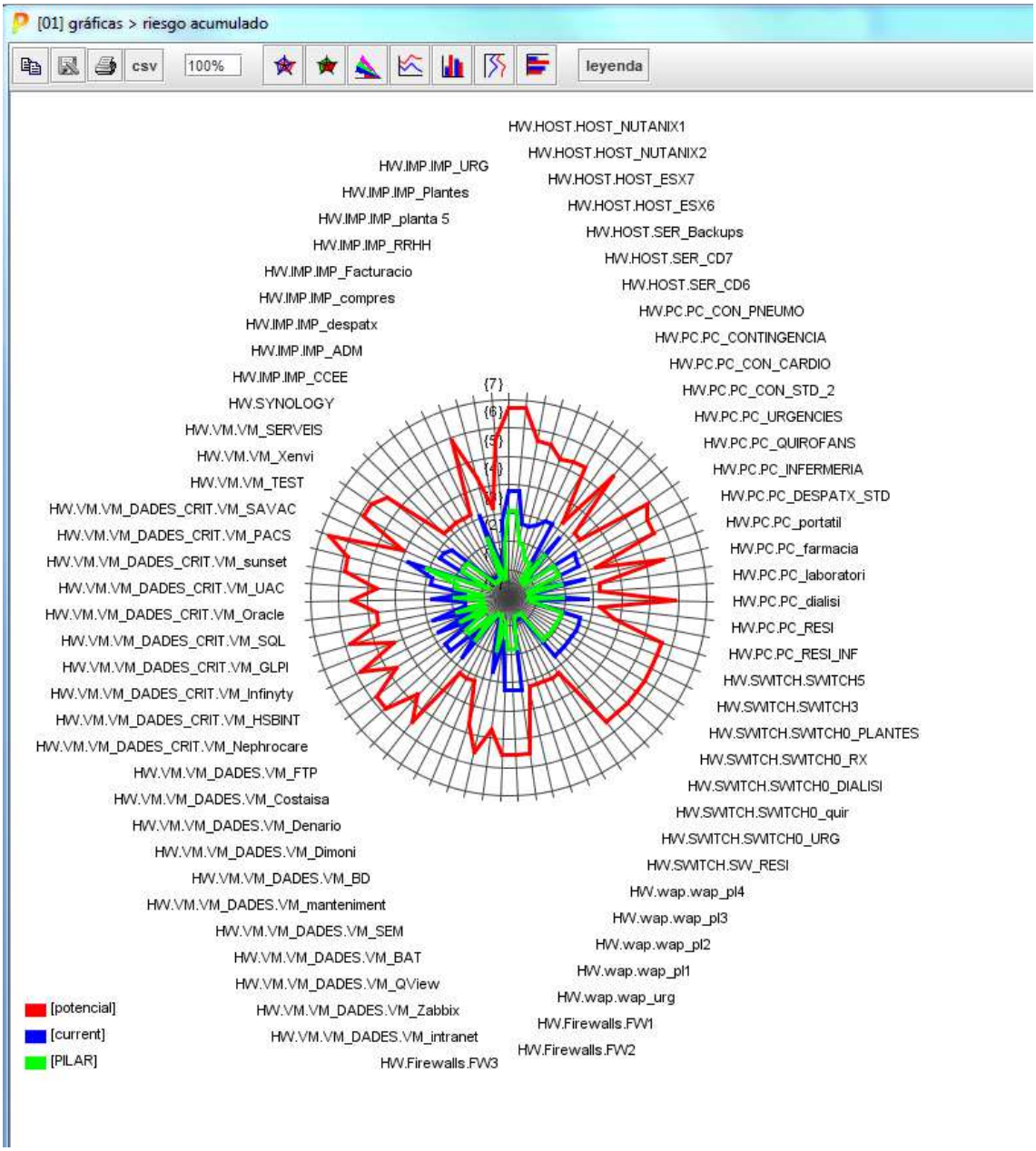
Es monitoritzen les aplicacions instal·lades amb el GLPI

Analitzar vulnerabilitats regularment

Projectes detectats punt 4.7

[PR01.47]Descriure processos de control de programari en el GLPI automatitzats i mesurables

4.8[HW] PROTECCIÓ DELS EQUIPS INFORMÀTICS



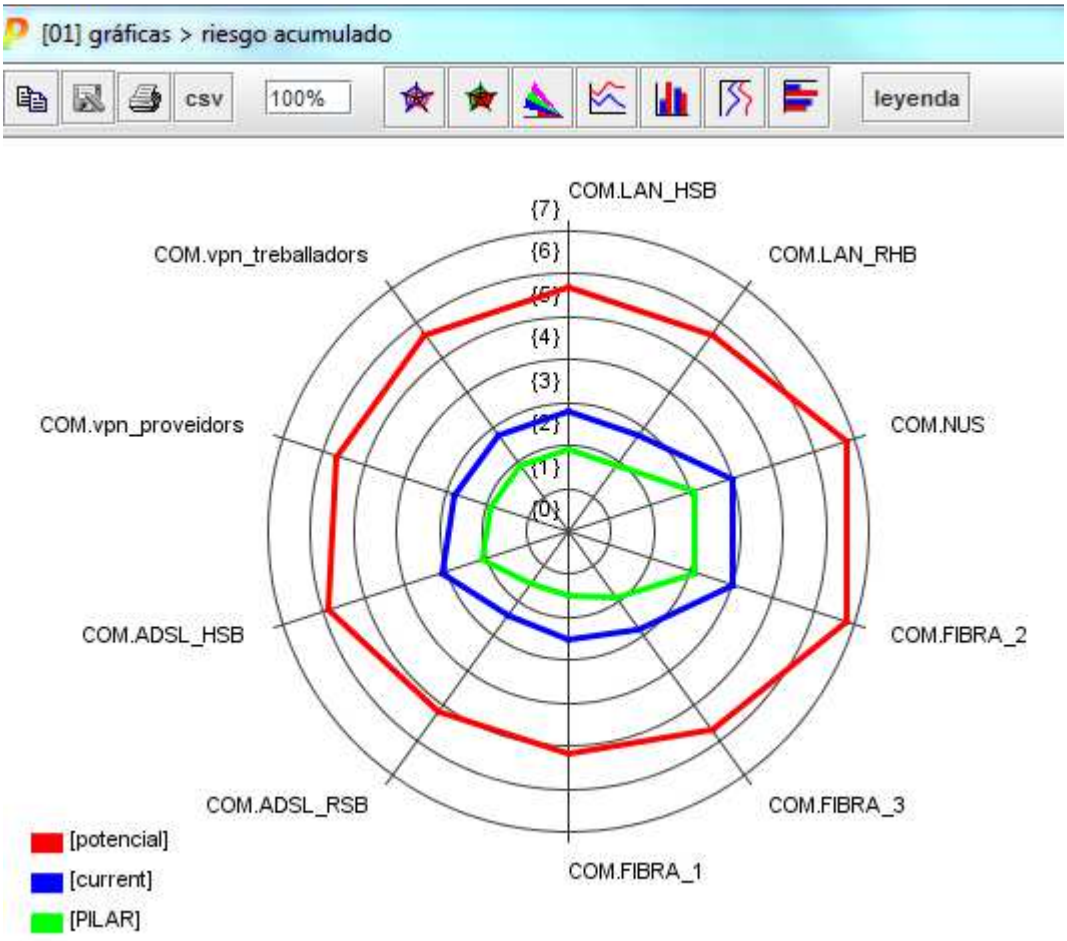
Els equips clients estan configurats d'una manera estàndard, i si el lloc on estan ubicats te risc de robatori s'asseguren amb cables i candaus Kensington.

Projectes detectats punt 4.8

[PR01.48] Redacció d'un estàndard de com inventariar els equips,de procediment d'us, de com passar a producció, de canvis i de desmantellament.

.

4.9[COM] PROTECCIÓ DE LES COMUNICACIONS



En la descripció de la Fundació es poden trobar els esquemes de comunicacions.

Projectes detectats punt 4.9

[PR01.49] Redacció d'un estàndard de com inventariar els telèfons mòbils,de procediment d'us, de com passar a producció, de canvis i de desmantellament.

[PR02.49] Redacció d'un estàndard de com inventariar VPN .

[PR03.49] Redacció d'un manual de com crear VPN i donar de baixa.

[PR04.49] Redacció d'un estàndard de com guardar les copies de configuració dels firewalls i els switch .

[PR05.49] Instal·lar programari de monitoritzacio de xarxa.

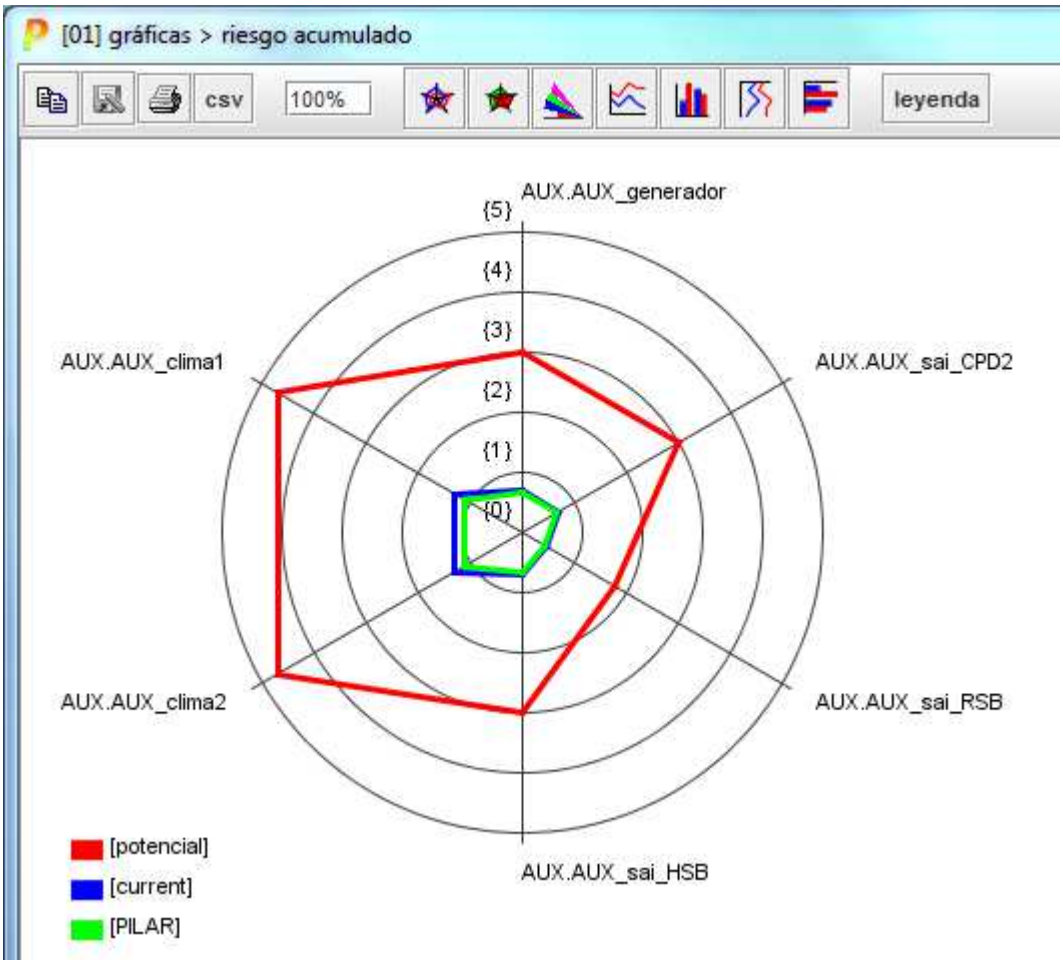
[PR06.49] Redacció d'un estàndard per teletreball .

[PR07.49] Redacció d'un estàndard sobre politiques del firewall .

[PR08.49] Millora de l'arquitectura de comunicacions externes, sobretot redundància de sortida a Internet per la Residencia.

[PR09.49] Redacció d'un control mesurable per revisar seguretat de la xarxa

4.10[AUX] ELEMENTS AUXILIARS



Els SAIS i els climes estan assegurats dintre dels CPD, el generador també es troba en un local a part protegit.

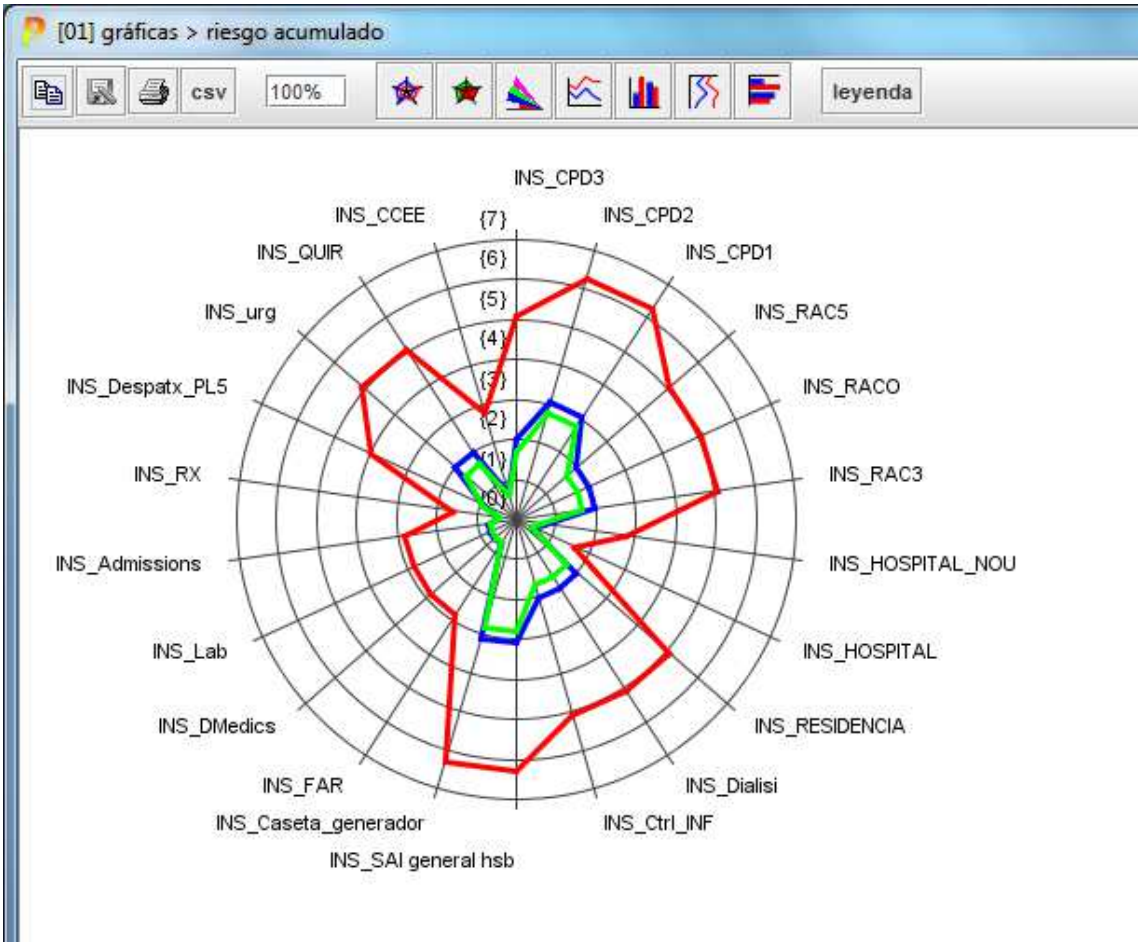
Els climes estan duplicats.

Podem observar en el gràfic que la línia blava que correspon a l'estat actual es superposa a la verda que es la recomanada per PILAR.

Projectes detectats punt 4.10

[PR01.410] Redacció d'un estàndard de com inventariar els elements auxiliars.

4.11[L] PROTECCIÓ DE LAS INSTAL·LACIONS



Podem observar en aquest gràfic com en l'anterior, que la línia blava que correspon a l'estat actual es superposa a la verda que es la recomanada per PILAR.

Les instal·lacions estan protegides contra el foc, existeix un pla de emergència i es forma al personal en aquests aspectes.

També hi ha un pla contra la violència i es disposa de botons de pànic en els consultoris mèdics.

Hi han detectors i filtres de legionel·la en els aires acondicionats i es fan proves periòdicament de l'esterilització dels quiròfans.

Falta reparar aparell registre entrades i càmera CPD1

Projectes detectats punt 4.11

[PR01.411] Reparar aparell entrada CPD 1

[PR02.411] Reparar càmera interior CPD1

4.12[IR] GESTIÓ D'INCIDENTS

A la fundació existeix un comitè de seguretat s'ha contractat un delegat de protecció de dades recentment i conte amb un registre de incidències que es valoren en el comitè.

També s'analitzen els projectes nous en quan a riscos de seguretat (DPD)

Projectes detectats punt 4.12

[PR01.412] Incloure en la intranet un apartat de formació i conscienciació de seguretat.

4.13[V] GESTIÓ DE VULNERABILITATS

No existeix cap eina de gestió de vulnerabilitat de les configuracions ni es fan proves de penetració.

Projectes detectats punt 4.13

[PR01.413]Caldria seleccionar un software per poder fer proves de penetració cada 3 mesos

[PR02.413]Caldria crear un control monitoritzable i medible.

4.14[G] ORGANITZACIÓ

La Fundació ja tenia politiques de seguretat anteriors i ha passat auditories de seguretat. Cal però fer una revisió per adaptar la nova llei RGPD i els canvis de arquitectura que s'han dut a terme.

Projectes detectats punt 4.14

[PR01.414] Revisió dels documents de seguretat de la Fundació .

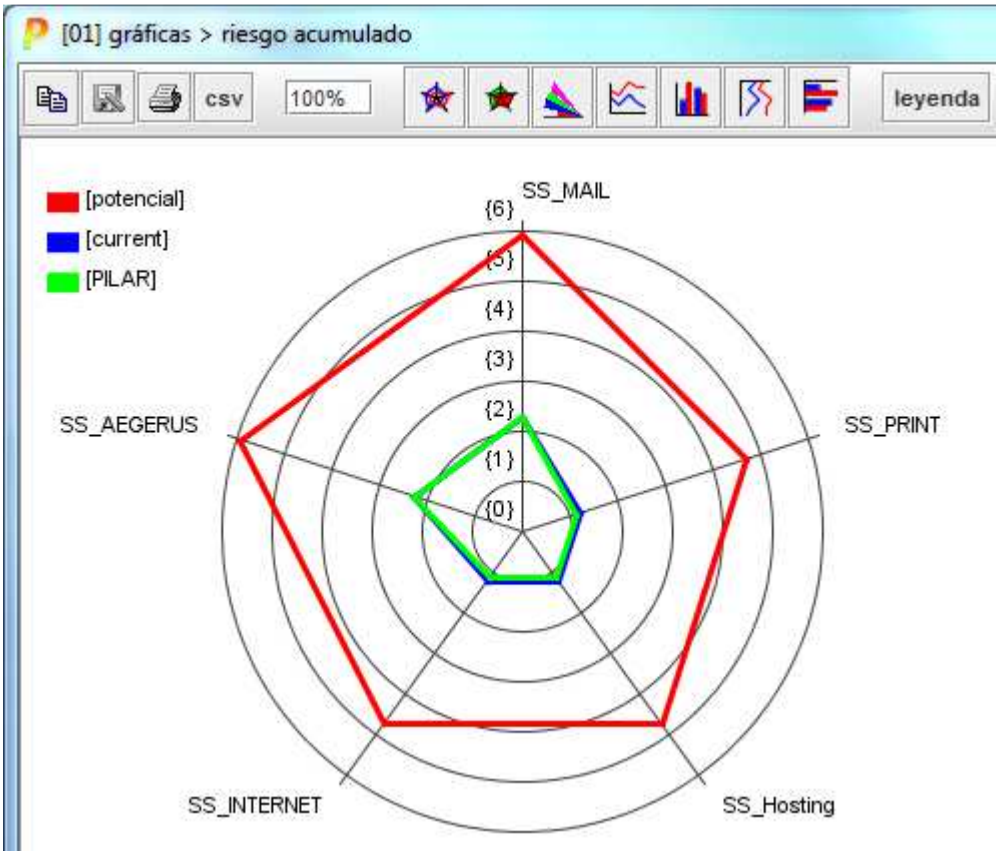
4.15[PPE] PROTECCIÓ FÍSICA DELS EQUIPS

Els servidors estan dins del CPD's tan el CPD 1 com el 2 estan protegits contra accessos indeguts, el CPD 3 no, esta a l'interior de la farmàcia de la Residencia i l'armari es pot obrir fàcilment.

Projectes detectats punt 4.15

[PR01.415]Caldria assegurar degudament el CPD3 contra accessos indeguts.

4.16[E] RELACIONS EXTERNES



Podem observar en aquest gràfic, que la línia blava que correspon a l'estat actual es superposa a la verda que es la recomanada per PILAR.

Les aplicacions externes estan protegides amb contractes SLA degudament comprovats pel DPD.

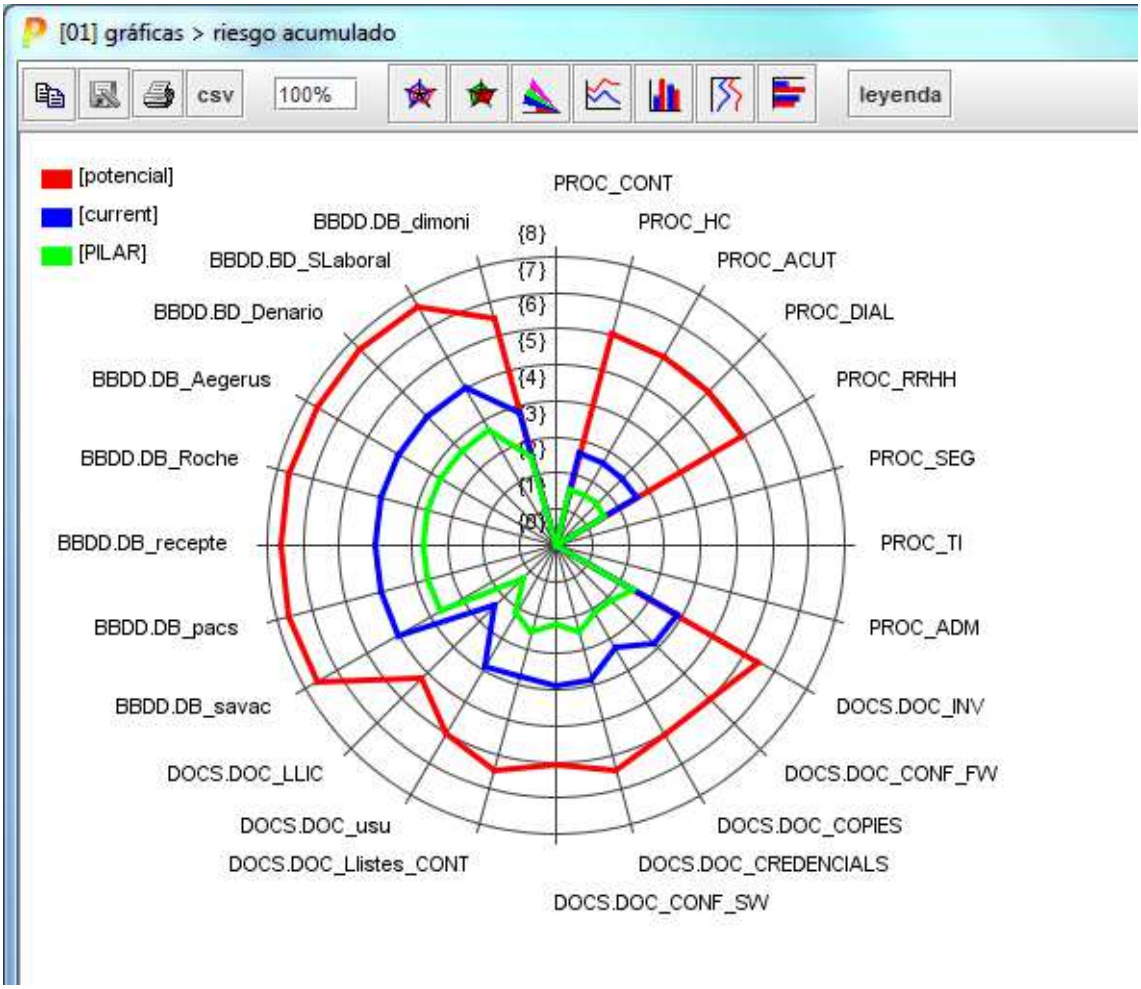
4.17 [NEW] ADQUISICIÓ /DESENVOLUPAMENT

Projectes detectats punt 4.17

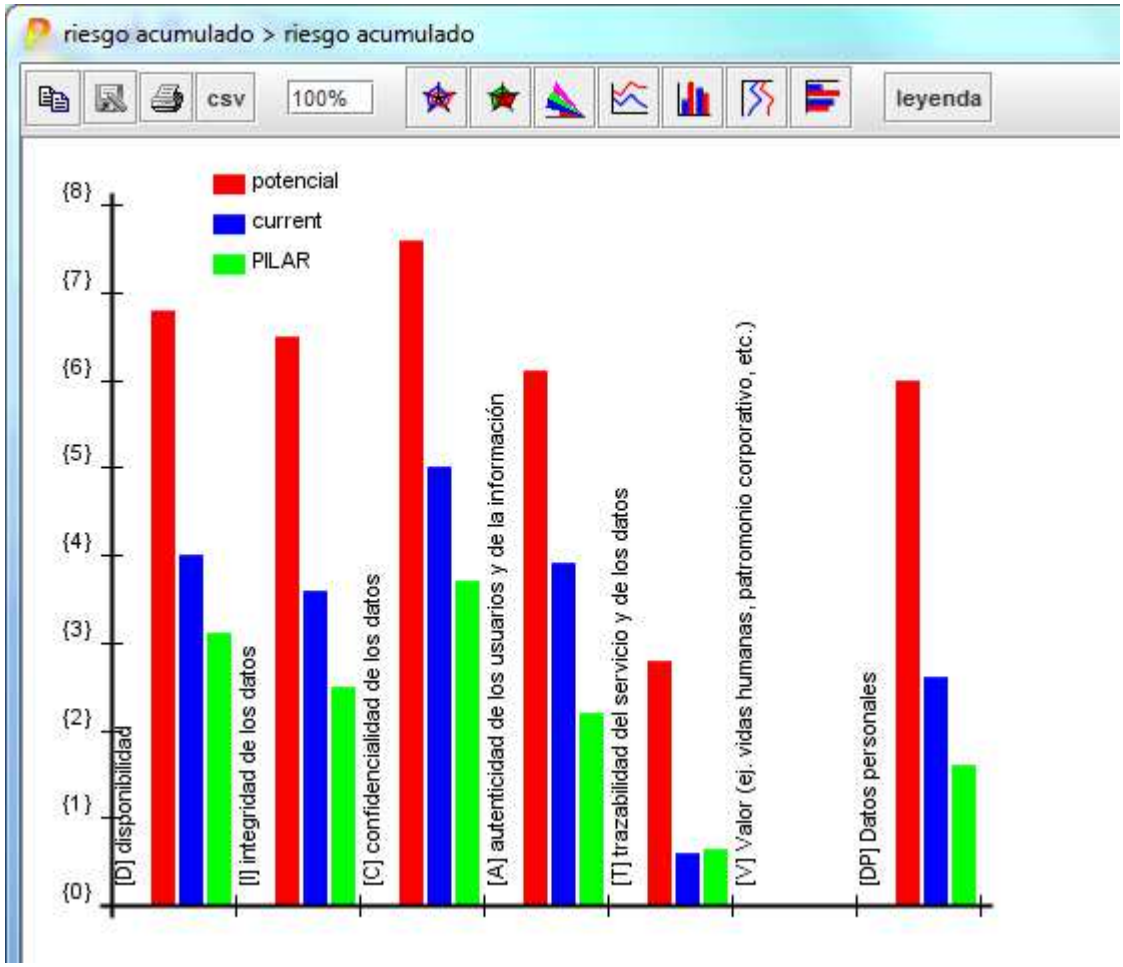
[PR01.417] Redacció d'un estàndard per adquirir software i equipament

[PR02.417] Redacció d'un estàndard sobre desenvolupament de programari segur.

ACTIUS ESSENCIALS



Risc acumulat per dimensió



Annexa 13 Pla de projectes

Annexa 14 - PLA DE PROJECTES

Avaluació de tots el projectes detectats, sorgits del resum executiu del Pla de Risc, que ha d'implementar l'organització per tal d'alinear-se amb els objectius del pla director, fent una quantificació econòmica i temporal del mateixos.

PROJECTES

[PR01.41]Projecte gestió documentació i expedients

[PR02.41]Projecte redacció normativa per utilitzar gestor documental i arxivar els arxius (etiquetatge, nivell seguretat, versions, informació autor, etc..)

[PR03.41]Redacció de un estàndard de metodologia de copies de seguretat i un control de les mateixes

[PR01.42]Projecte automatització de peticions per gestionar usuaris

[PR02.42]Projecte redacció i difusió estàndard, gestió altes baixes i modificacions d'usuaris i privilegis d'aquests.

[PR01.43]Caldria integrar l'accés a les aplicacions mes important al directory actiu per simplificar la gestió dels usuaris.

[PR01.44]Caldria copiar les configuracions de llocs de treball especials a la cabina de copies i crear una tasca de revisió de aquestes imatges cada 3 mesos o cada vegada que hi hagi un canvi.

[PR02.44]Caldria crear una wiki pels treballadors/es que utilitzen Aegerus a la residencia i afegir a la wiki del hospital les tasques de facturació, secretaria mèdica, comptabilitat, recursos humans.

Aquestes wikis s'haurien de revisar cada 6 mesos o cada vegada que hi hagin canvis.

[PR01.45]Caldria automatitzar i descriure el processos de control tan en l'antivirus com en els firewalls.

[PR01.46]Automatitzar i protocol·litzar els canvis de permisos i d'usuaris

[PR01.47]Descriure processos de control de programari en el GLPI automatitzats i mesurables

[PR01.48] Redacció d'un estàndard de com inventariar els equips,de procediment d'us, de com passar a producció, de canvis i de desmantellament

[PR01.49] Redacció d'un estàndard de com inventariar els telèfons mòbils,de procediment d'us, de com passar a producció, de canvis i de desmantellament.

[PR02.49] Redacció d'un estàndard de com inventariar VPN .

[PR03.49] Redacció d'un manual de com crear VPN i donar de baixa.

[PR04.49] Redacció d'un estàndard de com guardar les copies de configuració dels firewalls i els switch .

[PR05.49] Instal·lar programari de monitoritzacio de xarxa.

[PR06.49] Redacció d'un estàndard per teletreball .

[PR07.49] Redacció d'un estàndard sobre politiques del firewall .

[PR08.49] Millora de l'arquitectura de comunicacions externes, sobretot redundància de sortida a Internet per la Residencia.

[PR09.49] Redacció d'un control mesurable per revisar seguretat de la xarxa

[PR01.410] Redacció d'un estàndard de com inventariar els elements auxiliars.

[PR01.411] Reparar aparell entrada CPD 1

[PR02.411] Reparar càmera interior CPD1

[PR01.412] Incloure en la intranet un apartat de formació i conscienciació de seguretat.

[PR01.413]Caldria seleccionar un software per poder fer proves de penetració cada 3 mesos

[PR02.413]Caldria crear un control monitoritzable i medible de perill penetració.

[PR01.414] Revisió dels documents de seguretat de la Fundació .

[PR01.415]Caldria assegurar degudament el CPD3 contra accessos indeguts.

[PR01.417] Redacció d'un estàndard per adquirir software i equipament

[PR02.417] Redacció d'un estàndard sobre desenvolupament de programari segur

PROJECTES

Per facilitar la feina divideixo els projectes amb varies categories ,

- Redacció i revisió d'estàndards
- Creació i implantació de controls
- Implantació de nou programari
- Altres

REDACCIÓ I REVISIÓ ESTÀNDARDS(18)

[PR02.41]Projecte redacció normativa per utilitzar gestor documental i arxivar els arxius (etiquetatge, nivell seguretat, versions, informació autor, etc..)

[PR03.41]Redacció de un estàndard de metodologia de copies de seguretat i un control de les mateixes

[PR02.42]Projecte redacció i difusió estàndard, gestió altes baixes i modificacions d'usuaris i privilegis d'aquests.

[PR01.44]Caldria copiar les configuracions de llocs de treball especials a la cabina de copies i crear una tasca de revisió de aquestes imatges cada 3 mesos o cada vegada que hi hagi un canvi

[PR01.46]Automatitzar i protocol·litzar els canvis de permisos i d'usuaris *(s'inclourà en el [PR02.42])*

[PR01.48] Redacció d'un estàndard de com inventariar els equips,de procediment d'us, de com passar a producció, de canvis i de desmantellament

[PR01.49] Redacció d'un estàndard de com inventariar els telèfons mòbils,de procediment d'us, de com passar a producció, de canvis i de desmantellament.

[PR02.49] Redacció d'un estàndard de com inventariar VPN .

[PR03.49] Redacció d'un manual de com crear VPN i donar de baixa.

[PR04.49] Redacció d'un estàndard de com guardar les copies de configuració dels firewalls i els switch .

[PR06.49] Redacció d'un estàndard per teletreball .

[PR07.49] Redacció d'un estàndard sobre politiques del firewall .

[PR01.410] Redacció d'un estàndard de com inventariar els elements auxiliars.

[PR01.414] Revisió dels documents de seguretat de la Fundació .

[PR01.417] Redacció d'un estàndard per adquirir software i equipament

[PR02.417] Redacció d'un estàndard sobre desenvolupament de programari segur

[PR03.44] Redacció d'un estàndard de revisió i manteniment de wikis de coneixement.

CREACIÓ IMPLANTACIÓ DE CONTROLS(5)

[PR01.45]Caldria automatitzar i descriure el processos de control tan en l'antivirus com en els firewalls. * *es divideix en 2 controls AV i [PRO2.45] Firewalls*

[PR01.47]Descriure processos de control de programari en el GLPI automatitzats i mesurables

[PR09.49] Redacció d'un control mesurable per revisar seguretat de la xarxa

[PR02.413]Caldria crear un control monitoritzable i medible de perill penetració.

IMPLANTACIÓ DE PROGRAMARI(7)

[PR01.41]Projecte gestió documentació i expedients

[PR01.43]Caldria integrar l'accés a les aplicacions mes important al directory actiu per simplificar la gestió dels usuaris.

[PR02.44]Caldria crear una wiki pels treballadors/es que utilitzen Aegerus a la residencia i afegir a la wiki del hospital les tasques de facturació, secretaria mèdica, comptabilitat, recursos humans.

**Aquestes wikis s'haurien de revisar cada 6 mesos o cada vegada que hi hagin canvis.*

aquí afegeixo un nou projecte de redacció de estàndard [PR03.44]

[PR05.49] Instal·lar programari de monitoritzacio de xarxa.

[PR01.413]Caldria seleccionar un software per poder fer proves de penetració cada 3 mesos

[PR01.412] Incloure en la intranet un apartat de formació i conscienciació de seguretat.

[PR01.42]Projecte automatització de peticions per gestionar usuaris

ALTRES(2)

[PR08.49] Millora de l'arquitectura de comunicacions externes, sobretot redundància de sortida a Internet per la Residencia

[PR01.415]Caldria assegurar degudament el CPD3 contra accessos indeguts.

[PR01.411] Reparar aparell entrada CPD 1
[PR02.411] Reparar càmera interior CPD1

PLANIFICACIÓ

S'encarrega la responsabilitat de redacció dels documents a persones concretes i es revisaran a la comissió de seguretat i s'enviaran al DPD per revisió final, una vegada aprovats es presentaran a direcció per aprovació definitiva i es difondran als interessats.

Es calcula el temps que pot portar la feina però dependrà també de la disponibilitat de la persona.

REDACCIÓ I REVISIÓ ESTÀNDARDS

		QUI?	Hores treball
[PR02.41]	Gestor documental	Sec.Tècnica , CIO	7 hores
[PR03.41]	Copies seguretat	Adm. Sistemes, CIO	4 hores
[PR02.42]	Gestió comptes usuaris	RRHH, CIO	2 hores
[PR01.44]	Imatges lloc treball especials	Adm. Sistemes, CIO	1/2 hora
[PR01.49]	Gestió tel. Mobil	Adm. Sistemes, CIO	1 hora
[PR01.48]	Gestió pc client	Adm. Sistemes, CIO	1 hora
[PR02.49]	Gestió VPN	Adm. Sistemes, CIO	1 hora
[PR03.49]	Manual creació VPN	Adm. Sistemes,	2 hores
[PR04.49]	Gestió copies configuracions	Adm. Sistemes, CIO	1 hora
[PR06.49]	Gestió Teletreball	RRHH, CIO	3 hores
[PR07.49]	Politiques firewalls	Adm. Sistemes, CIO	1 hora
[PR01.410]	Inventari elements auxiliars	CIO	1 hora
[PR01.414]	Revisió doc. anterior sobretot pla de contingència	CIO,	1 setmana
[PR01.417]	Gestió adquisicions	CIO	3 hores
[PR02.417]	Programari segur desenvolupament	Desenvolupador, CIO	6 hores
[PR03.44]	Revisió wikis	Formació, CIO	1 setmana

CREACIÓ IMPLANTACIÓ DE CONTROLS

		QUI?	Hores treball
[PR01.45]	Control AV	Adm. Sistemes, CIO	5
[PR02.45]	Control FW	Adm. Sistemes, CIO	5
[PR01.47]	Control programari	Desenvolupador, CIO	5
[PR09.49]	Control xarxa	Adm. Sistemes, CIO	5
[PR02.413]	Control vulnerabilitat	Adm. Sistemes, CIO	5

PROGRAMARI

		QUI?	Hores treball
[PR01.41]	Gestor documental	CIO, Adm.BBDD,	15 dies, implantació i administració de Alfresco v.community - formació
[PR01.42]	Petic. creació usuaris	Adm.BBDD	3 dies, formulari en el GLPI
[PR01.43]	Integració a AD - SAVAC	SAVAC	Demanat a manteniment Savac
	Integració a AD - DENARIO	DENARIO	Demanat a manteniment Denario
	Integració a AD - AEGERUS	AEGERUS	Demanat a manteniment Aegerus
[PR01.412]	Intranet-concienciacio seg	CIO, Comunicació	Intranet (Drupal) , desenvolupament mòdul , 3 dies
[PR02.44]	Wiki aegerus	Desenvolupador, Personal residencia	Desenvolupat amb mediawiki 1 setmana
	Wiki facturació	Desenvolupador, Personal facturació	Desenvolupat amb mediawiki 2 setmanes
	Wiki sec mèdica	Desenvolupador, Personal Sec Mèdica	Desenvolupat amb mediawiki 1 setmana
	Wiki comptabilitat	Desenvolupador, Personal comptabilitat	Desenvolupat amb mediawiki 1 setmana
	Wiki RRHH	Desenvolupador, Personal RRHH	Desenvolupat amb mediawiki 2 setmanes
[PR05.49]	Monitor xarxa	Adm. Sistemes	Es requereix primer un estudi per decidir quina eina utilitzar 2 setmanes
[PR01.413]	Escàner vulnerabilitats	Adm. Sistemes	2.565€/any llicencia, 3 setmanes (Nessus prof)

ALTRES

		QUI?	Hores treball
[PR08.49]	Arquitectura comunicacions- redundància Internet Residencia	Estudi encarregat a telefònica	1 mes
[PR01.415]	Millora CPD3	Equip sitic	2 setmanes
[PR01.411]	Reparació	Empresa externa	1 setmana
[PR02.411]	Reparació	Empresa externa	1 setmana

COST APROXIMAT DELS PROJECTES

La majoria de projectes els portarà a terme el propi equip de sistemes de la fundació juntament amb altre personal de l'empresa.

En aquest cas el cost es de personal propi.

El Gestor documental que es vol implantar no te cost de llicencia però si que portarà associat un cost en hores de personal , tan de implantació com de formació .

S'ha fet un càlcul de les hores totals i del personal implicat .

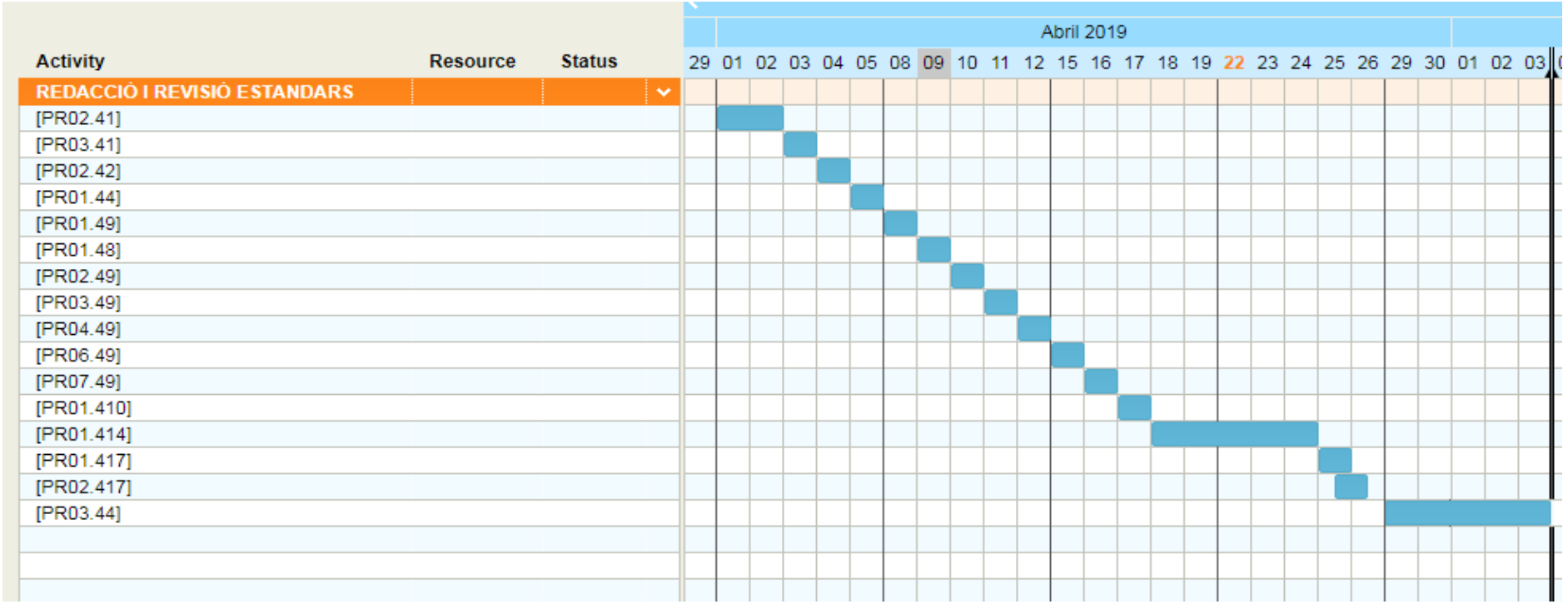
Persona	**Hores**
CIO	110 Hores
Adm Sistemes	60 hores
Desenvolupador	60 hores
Administrador BBDD	40 hores

En algun projecte si que s'han de sumar costos de llicencies de programari i en altres de pressupostos que es demanaran a l'empresa que els porti a terme.

Escàner vulnerabilitats	Nessus Professional	2.565€/any llicencia

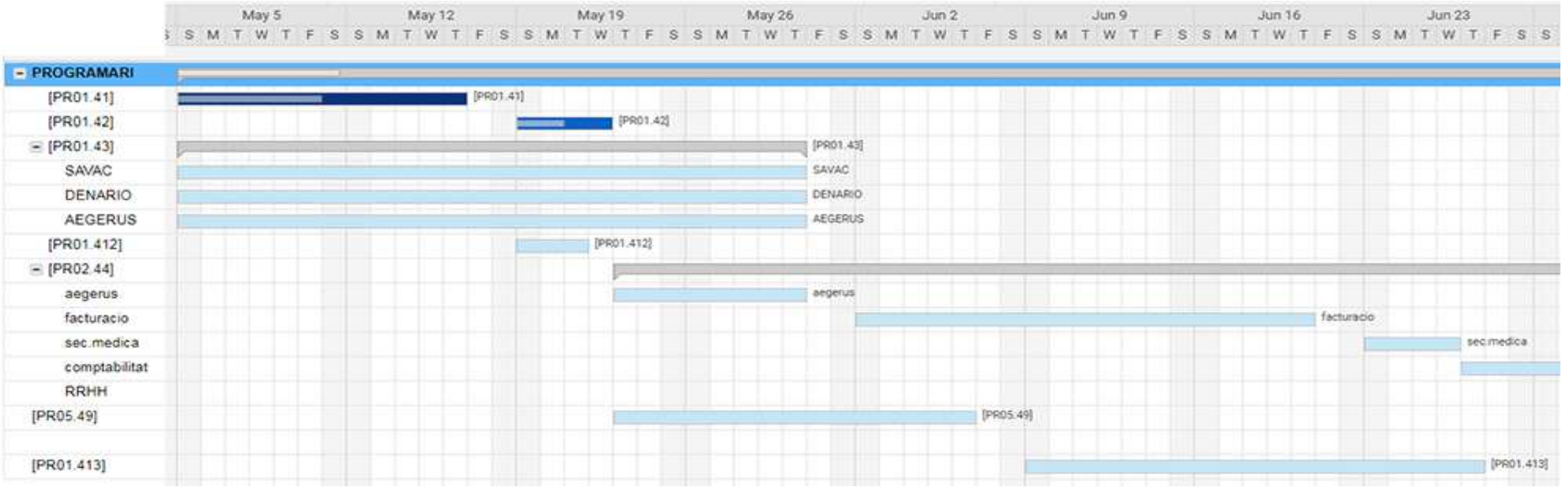
Integració a AD - SAVAC	SAVAC	S'ha de demanar pressupost a SAVAC
Integració a AD - DENARIO	DENARIO	S'ha de demanar pressupost a Denario
Integració a AD - AEGERUS	AEGERUS	S'ha de demanar pressupost a Aegerus
Reparació	Empresa externa	S'ha de demanar pressupost
Reparació	Empresa externa	S'ha de demanar pressupost
Arquitectura comunicacions-redundància Internet Residencia	Estudi encarregat a telefònica	S'ha de demanar pressupost a telefònica

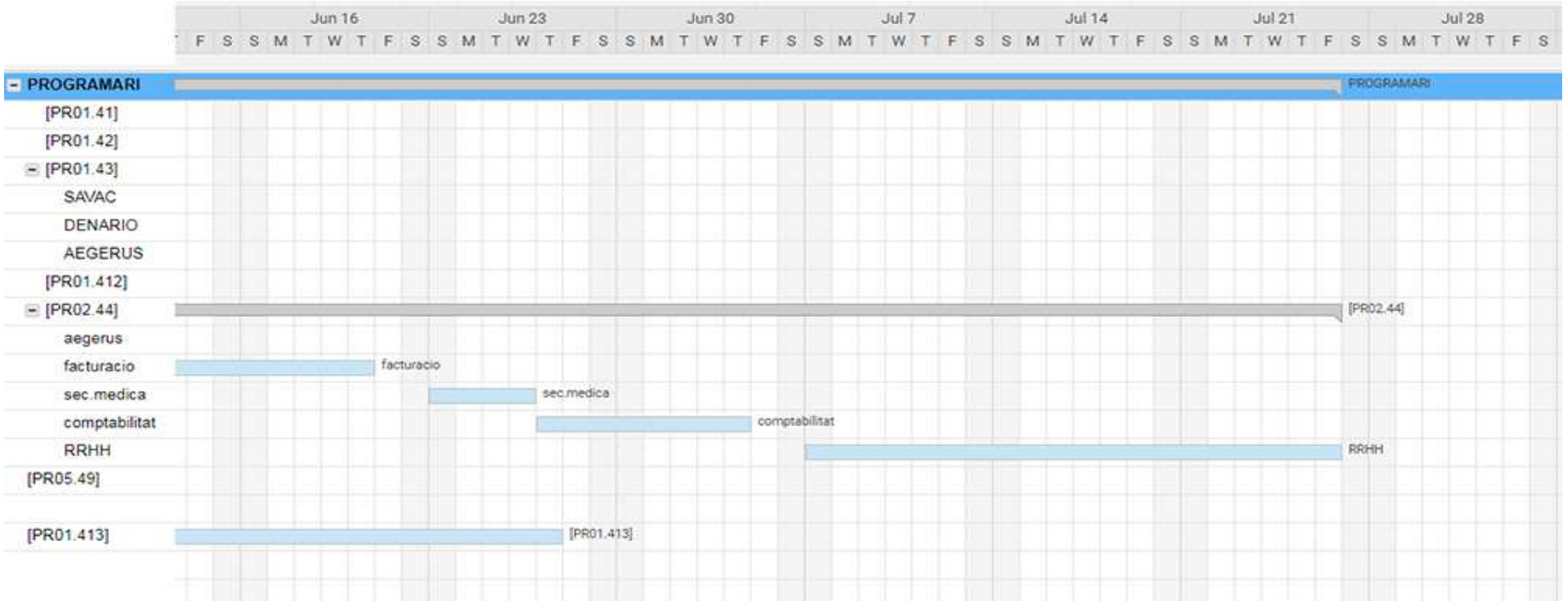
Projectes de redacció i revisió de estàndard



Nombre de la tarea	Fecha de Inicio	Fecha final	Asignado a
PROGRAMARI	**05/05/19**	**26/07/19**	
[PR01.41]	05/05/19	16/05/19	A Adm.Sistemes C CIO
[PR01.42]	19/05/19	22/05/19	Adm.Sistemes
[PR01.43]	05/05/19	30/05/19	
SAVAC	05/05/19	30/05/19	S savac
DENARIO	05/05/19	30/05/19	D denario
AEGERUS	05/05/19	30/05/19	A aegerus
[PR01.412]	19/05/19	21/05/19	C CIO
[PR02.44]	23/05/19	26/07/19	P programador
aegerus	23/05/19	30/05/19	
facturacio	02/06/19	20/06/19	
sec.medica	23/06/19	26/06/19	
comptabilitat	27/06/19	04/07/19	
RRHH	07/07/19	26/07/19	
[PR05.49]	23/05/19	06/06/19	A Adm.Sistemes
[PR01.413]	09/06/19	27/06/19	A Adm.Sistemes

Projectes de instal·lació o configuració programari

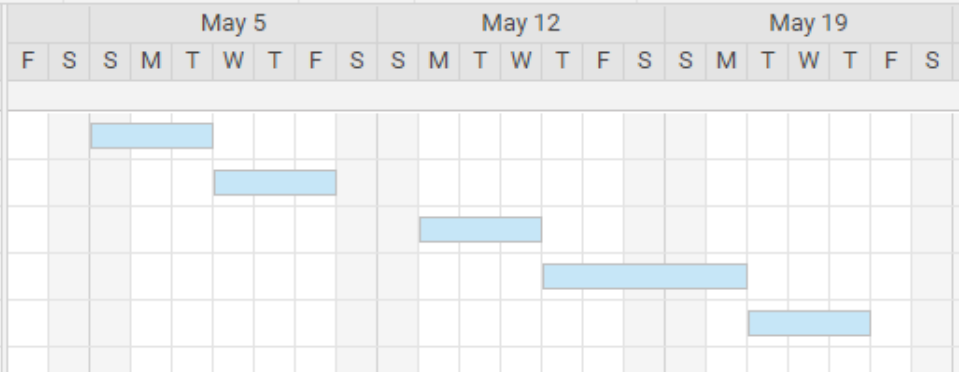

May 5
May 12
May 19
May 26
Jun 2
Jun 9
Jun 16
Jun 23
PROGRAMARI
[PR01.41]
[PR01.42]
[PR01.43]
SAVAC
DENARIO
AEGERUS
[PR01.412]
[PR02.44]
aegerus
facturacio
sec.medica
comptabilitat
RRHH
[PR05.49]
[PR01.413]



Annexa 13 Pàgina 12 (de 16)

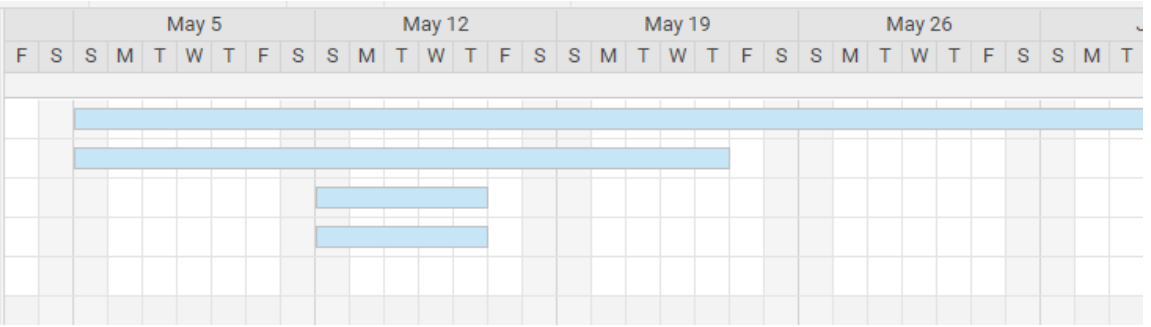
Projectes d'implantació de controls

Implantar controls	Duration	Start	Finish	Autor
[PR01.45]	3d	05/05/19	07/05/19	Adm.Sistemes
[PR02.45]	3d	08/05/19	10/05/19	Adm.Sistemes
[PR01.47]	3d	13/05/19	15/05/19	programador
[PR09.49]	3d	16/05/19	20/05/19	Adm.Sistemes
[PR02.413]	3d	21/05/19	23/05/19	Adm.Sistemes



Altres projectes

Altres	Duration	Start	Finish	asignat
[PR08.49]	30d	05/05/19	13/06/19	Telefonica
[PR01.415]	15d	05/05/19	23/05/19	Equip SITIC
[PR01.411]	5d	12/05/19	16/05/19	Empresa externa
[PR02.411]	5d	12/05/19	16/05/19	Empresa externa



A continuació s'adjunta una plantilla que servirà per escriure els ESTÀNDARDS i una altre pels PLANS DE CONTINGÈNCIA.

	[Tipus d'estàndard]* Tipus+nom				**[Codificació]** Tipus+versió+num
	[versió]	**[difusió]**	Data creació		[protecció] Creative commons
	[estat] Aprovat, revisió,discussió	[autors]	Data revisions		n.pag/n.total pag

TÍTOL

- Objectiu (causa)
- Àmbit (a qui va dirigit)
- Recurs afectat
- Compliment legal (Ex ISO 27002)
- Descripció (mesures de seguretat de mes a menys)
- Control (qui farà control i com)
- Seguiment periòdic
- Auditoria
- Penalitzacions
- Divulgació
- Responsable
- Mitjans de divulgació
- Revisió (data i/o causes de revisió)
- Glossari de termes
- Documentació referenciada
- Paraules clau
- Grup de treball i aprovació

** **Politiques** : directrius estratègiques de alt nivell, pot ser primer i segon nivell, compliment obligatori, dirigit a tot el personal*

***Norma -guia**: procés homogeni per una determinada necessitat, optimitza recursos, desenvolupa una política, compliment obligatori la norma, la guia es una recomanació de bones practiques, divulgació al personal específic.*

***Procediment** : Conjunt d'accions per aconseguir un objectiu, compliment obligatori, normalment intervé mes d'un departament, divulgació als implicats, aprovat pel responsable.*

***Manual o instruccions** : desenvolupen normes o guies , son llistes de tasques o instruccions detallades per fer accions determinades o per utilitzar eines concretes, solen dependre del entorn tecnològic canvien al fer canvis de productes o de versió. Divulgació a les persones interessades aprovades pel responsable.*

- Objectiu. (que es pretén aconseguir, quina funció te aquest pla)
- Abast (serveis que es pretenen garantir, les localitzacions, personal afectat)
- Descripció de la situació que cal controlar:
  - Riscos que s'han de controlar(amenaces)
  - Actius que hi intervenen (actius)
  - Nivell de servei exigit (mínims)
  - Temps per a cada resposta: temps total de reacció.
  - Recursos necessaris en cadascun dels plans.
  - Disponibilitat i operativitat.
- Llista de procediments concrets (i responsables d'aquests procediments)
- Disparament d'alarma.(quant comencem a utilitzar el pla, responsable d'avisar)
- Pla de resposta. (conjunt d'accions que es fan immediatament després del disparament de l'alarma de contingència)
  - Accions per a protegir les persones
  - Accions per a tallar la situació de risc: control de les amenaces
  - Accions per a protegir els actius.
  - Accions de notificació pública
  - Registre de les accions que es duen a terme.
- Pla de suport.
  - Recursos necessaris per a mantenir l'operació
  - Manteniment dels recursos.
  - Activació de les diferents accions (persona encarregada)
  - Identificació del personal implicat.
  - Registre de les accions dutes a terme: inici, desenvolupament i resultats.
- Pla de recuperació.
  - Restitució d'actius, subministraments, entorn.
  - Arrencada dels sistemes, serveis,etc.
  - Proves per a comprovar els sistemes restaurats.
  - Posada en operació
  - Retirada dels plans de suport.
  - Registre de les accions fetes i dels resultats.

annexa 15

2019

INFORME D'AUDITORIA

Informe nº 2019-3-54

UOC MISTIC

Auditoria realitzada

Montserrat Magnet Sabata

Resum executiu

Auditoria de compliment de la norma ISO 27001:2013 de la Fundació Hospital Sant Bernabé de Berga

Data : 01/04/2019

Abast : SGSI de la Fundació

Tipus d'auditoria : Auditoria interna

Auditors : Montserrat Magnet, David Butxaca, Anna Rodríguez

Una vegada realitzada l'auditoria s'ha trobat un grau de maduresa en quant al sistemes de gestió de la seguretat del 90,42 % sobre un 100% , el que indica un grau òptim.

S'han detectat algunes "No conformitats menors" que indiquen discrepància respecte algun punt concret d'un domini però no, del domini complert.

Les normes Iso 27001 estan dividides en dominis, son aspectes amplis d'organització de la seguretat i cada un d'aquests dominis, esta dividit en punts mes concrets.

En especial s'ha donat importància i s'ha etiquetat com a Nivell 4 (important) , la NC3, i la NC5 aquestes s'haurien de solucionar en quan fos possible.

La NC3 es refereix al suports físic en transit es a dir, quan un ordinador portàtil o un smartphone surten de la seva seu, en el seu interior pot haver-hi informació confidencial de la Fundació, per aquest motiu s'hauria de protegir aquesta per tal de que en cas de pèrdua o robatori del aparell no es pogués arribar a obtenir.

Aconsellem encriptar-la amb un algoritme robust ja siguiu tot el disc dur o nomes la part confidencial dels portàtils i de la memòria dels smartphones.

La NC5 missatgeria electrònica,es deguda a que no hi ha copies de seguretat de aquesta missatgeria, en cas de desastre, no es podrien recuperar els correus importants que podrien ser decisius per la Fundació.

S'aconsella implantar un programa de copies de seguretat en aquesta missatgeria o un canvi de pla office 365 (actualment esta implantat el pla Quiosc) , per un que inclogui aquestes copies.

De Nivell 3 , Moderadament important , s'ha trobat alguna no conformitat en el procés de contractació (NC2), caldria investigar els antecedents del personal que es contracta de nou i registrar els canvis en els drets d'accés dels usuaris (NC4).

També s'aconsella desabilitar amb algun programa MDM (Mobile Device Management) l'accés a les xarxes wifi, des de els smartphones que s'entreguen als treballadors. L'accés a les xarxes publiques es molt perillós, podem exposar-nos sense necessitat a

una sèrie de riscos com robament de dades emmagatzemades, robament de dades en transit i infecció del dispositiu .

Una altra no conformitat de nivell 3 son les restriccions als canvis en els paquets de programari, s'ha detectat que alguns programes poden actualizar-se sense intervenir l'administrador .

Com a fortalesa, destacar l'alta puntuació del domini "gestió d'incidents de seguretat", i de la "gestió de la continuïtat del negoci".

La gestió d'incidents esta ben documentada i de cada incident se'n treuen conclusions que es documenten, s'aprèn de les situacions generades.

La continuïtat del negoci esta també ben dimensionada, des de varies perspectives, els supòsits de desastres on s'haurien d'aplicar les politiques de continuïtat deixen un marge de risc residual molt baix i donen elements de suport i solucions a les situacions descrites amb l'única excepció de les copies de seguretat del correu electrònic explicada anteriorment.

Definició de l'auditoria

Objectiu de l'auditoria

L'objectiu de l'auditoria, es l'anàlisi de compliment de l'organització davant la norma ISO: IEC 27001:2013 de la Fundació Hospital Sant Bernabé,comprovant que l'SGSI que esta implantat compleix amb els requisits de la norma i que els processos de l'organització han integrat correctament els requisits de seguretat de la informació que defineix l'SGSI.

Es una auditoria interna en què es verificarà el compliment tant dels requisits propis de l'empresa,com els requisits de la norma ISO27001:2013 i que serà preparatòria per una auditoria de certificació.

L'eix central de la ISO 27001 és protegir la confidencialitat, integritat i disponibilitat de la informació en una empresa, Investigant quins són els potencials problemes que podrien afectar la informació (és a dir, l'avaluació de riscos) i després definint el que cal fer per evitar que aquests problemes es produeixin (és a dir, mitigació o tractament del risc).

Abast de l'auditoria

Te com Abast, el mateix del Sistema de gestió de seguretat de la informació (SGSI) de La Fundació Hospital Sant Bernabé es a dir, els processos i les infraestructures que abasta el SGSI en especial els mes crítics i els mes vulnerables.

L'abast esta definit d'acord amb varis aspectes:

- Processos i serveis principals
- Unitats organitzatives, s'inclouen, totes les unitats de caire assistencial i de suport a aquest, s'exclouen les unitats de menjador, neteja, servei religiós
- Ubicacions. tots els espais que alberguen físicament els mitjans amb què es tracten les dades, i aquells que serveixen directa o indirectament per a accedir al/s fitxer/s.
- Les Xarxes i infraestructura de TI tan de l'Hospital com de la Residencia Sant Bernabé

Modalitat d'auditoria

Auditoría interna.

L'auditoria interna serveix com a preparació per a l'auditoria de certificació i per validar l'efectivitat del SGSI implantat , no només per avaluar el compliment amb els requisits de l'SGSI que és l'objecte més directe de l'auditoria de certificació es també una eina d'informació per a l'objectiu de la millora contínua

En aquesta auditoria s'han analitzat aspectes organitzatius tècnics i físics

Planificació de l'auditoria

Equip Auditor

Montserrat Magnet Sabata,enginyer informàtic col·legiat nº 85789, Responsable de Seguretat i director del departament de sistemes i auditor intern expert com a Director de l'auditoria , responsable de dirigir l'auditoria i redactar l'informe final.

David Butxaca , enginyer informàtic Col·legiat nº 58698, Responsable de sistemes d'informació

Responsable d'auditar processos orientats a TI:

A.9 Control d'accés
A.10 Criptografia
A.11 Seguretat física i ambiental
A.12 Seguretat operacional
A.13 Seguretat de les comunicacions
A.14 Adquisició, desenvolupament i manteniment del sistema

Anna Rodriguez , com a membre de comitè de seguretat i secretaria tècnica

Responsable de requisits generals:

A.5 Polítiques de seguretat de la informació
A.6 Organització de la seguretat de la informació
A.7 Seguretat dels recursos humans
A.8 Gestió d'actius
A.15 Relacions del proveïdor
A.16 Gestió d'incidents de seguretat de la informació
A.17 Aspectes de seguretat de la informació de la gestió de la continuïtat del negoci
A.18 Compliment

Participants en el procés d'auditoria

Gerència de la Fundació, com a responsable final de tota la seguretat .

Directora d'infermeria com a responsable de tècniques assistencials i funcionals.

Directora de Recursos Humans com a responsable de contractació i formació del personal.

Responsable de manteniment com a responsable de seguretat física del perímetre i de manteniment d'infraestructures.

Documentació de referència

- Política de seguretat de l'empresa annexa 6 del SGSI
- Pla d'auditoria annexa7 del SGSI
- Resultats dels registres de controls definits en l'annexa 8 del SGSI
- Annexa 14, (normatiu) ISO 27001: 2017 , SGSI
- Annexa 15, No conformitats detectades
- Annexa 16, Documentació auditada
- Pla d'auditoria

Metodologia emprada

S'ha seguit el recomanat a *ISO27k_ISMS_internal_audit_procedure* del autor Richard O. Regalado i Fòrum ISO27k modificat i millorat per adaptar-se a les necessitats d'aquesta organització.

Estàndards

Sa utilitzat la norma ISO 27001 que és una norma internacional emesa per l'Organització Internacional de Normalització (ISO) i descriu com gestionar la seguretat de la informació en una empresa.

La revisió més recent d'aquesta norma va ser publicada el 2013 i ara el seu nom complet és ISO / IEC 27001: 2013.

La primera revisió es va publicar en 2005 i va ser desenvolupada d'acord amb la norma britànica BS 7799-2.

Fases

S'han portat a terme 5 fases,

Fase 1 revisió de la documentació y planificació de la auditoria

- auditar que els documents del sistema de gestió requerits per la norma estan disponibles i implantats
- auditar que hi ha un compromís i alineació de l'alta direcció amb els objectius de negoci del SGSI
- auditarem que els controls seleccionats són apropiats

Fase 2 auditoria inicial i visita de auditoria a les àrees auditades de la Fundació, Hospital i Residencia

- avaluació dels processos d'anàlisi de riscos i el seu tractament, validació de les interfases i dependències no incloses en el abast,
- avaluació de les polítiques, els objectius, els programes i els procediments i que s'han implantat de manera eficaç
- revisar la posada en pràctica de les disposicions de mesurament i monitoratge per auditar el funcionament del sistema de gestió i si es estan assolint els objectius.

Fase 3 realització d'entrevistes al personal afectat

Fase 4

- auditar si s'ha dut a terme almenys una revisió per la direcció
- si hi ha un enfocament cap a la millora planificada i sistemàtica

Fase 5

- redacció de l'informe d'auditoria i presentació a la direcció

Tècniques

1-Chec list documentacions requerides

2- reunions amb els responsables dels departaments

3- avaluació de registres de controls de seguretat

4- visites a les àrees afectades

Terminis

Tal com estava previst en el Pla d'auditoria , les proves es van desenvolupar la primera quinzena de març del 2019.

En el document de cada prova hi consta el dia concret.

Resultats de l'auditoria

S'han re-calculat els valors dels dominis de la Iso 27001, una vegada executat el Pla de projectes de seguretat.

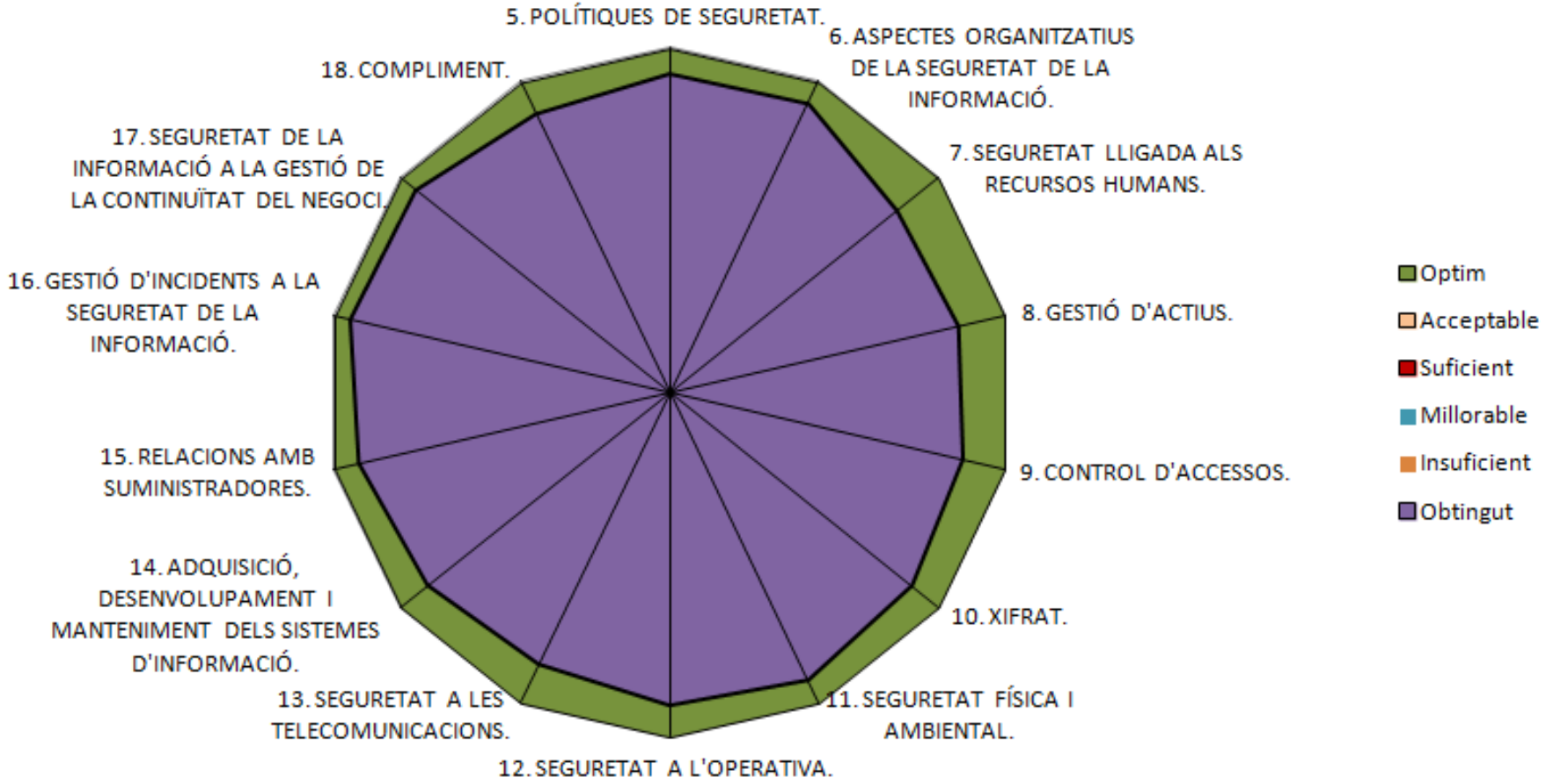
Es poden consultar els resultats desglossats a l'Annexa 17

Els valors obtinguts actuals son els següents :

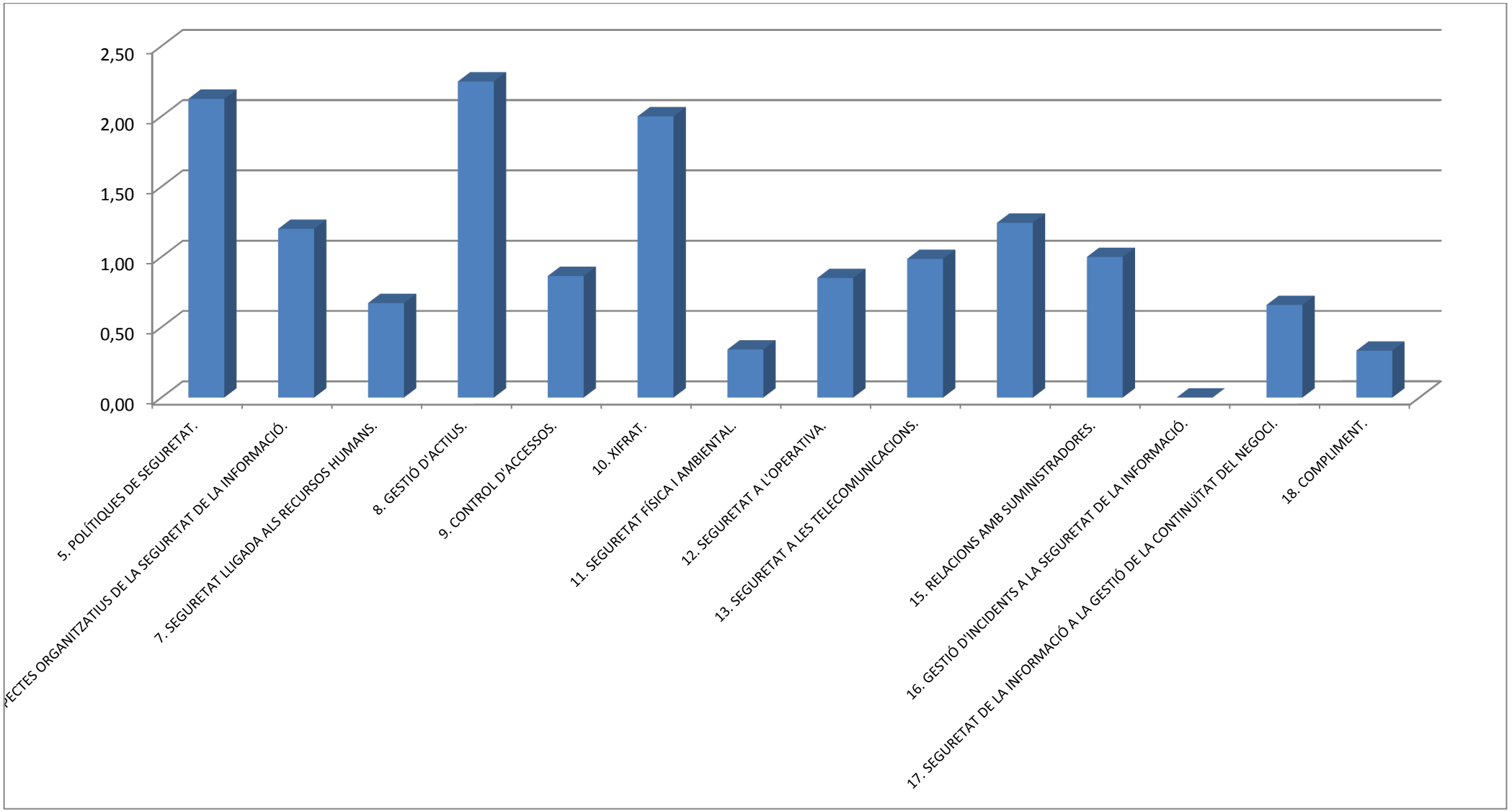
	Valor
5. POLÍTIQUES DE SEGURETAT.	4,63
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	4,65
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS.	4,22
8. GESTIÓ D'ACTIUS.	4,30
9. CONTROL D'ACCESSOS.	4,36
10. XIFRAT.	4,50
11. SEGURETAT FÍSICA I AMBIENTAL.	4,64
12. SEGURETAT A L'OPERATIVA.	4,55
13. SEGURETAT A LES TELECOMUNICACIONS.	4,39
14. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ.	4,49
15. RELACIONS AMB SUMINISTRADORES.	4,63
16. GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	4,75
17. SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.	4,71
18. COMPLIMENT.	4,48
Promig	4,52

El nivell de maduresa del sistema en base als controls exposats és de 4.53 (90,42%) OPTIM, situant el sistema i el resultat d'aplicar els projectes de millora de la seguretat com a mesures efectives i suficients que impliquen un increment de l'estat de seguretat i assoleixen l'objectiu de compliment proposat per l'empresa.

Nivell de maduresa actual



Augment dels nivells dels diferents dominis



No conformitats

Amb aquesta auditoria s'han detectat les següents no conformitats, d'acord amb el grau de compliment de la norma per als següents controls:

Nivell 2

18.1.5 Regulació dels controls criptogràfics

Nivell 3

NC2 7.1 Abans de la contractació.
NC2 7.1.1 Investigació d'antecedents.
NC4 9.2.5 Revisió dels drets d'accés dels usuaris.
NC4 9.2.6 Retirada o adaptació dels drets d'accés
NC6 14.1.2 Seguretat de les comunicacions en serveis accessibles per xarxes públiques
NC7 14.2.4 Restriccions als canvis en els paquets de programari.

Nivell 4

NC3 8.3.3 Suports físics en trànsit..
NC5 13.2.3 Missatgeria electrònica.

Les no conformitats menors indiquen una discrepància respecte a un punt d'un domini de la norma. Les majors en canvi indicarien una falta de incompliment d'un domini complet

No s'ha trobat cap "No conformitat major "

Annexes

Annexa 16: No conformitats detectades

Annexa 17 : Revisio de la documentació

Annexa 18: (normatiu) ISO 27001: 2017

Annexa 16- Auditoria UOC2019MMS: No conformitats detectades

No conformitat	*Auditor*	*Data*
NC2	A.Rodriguez	4/03/2019

Descripció

Es demana a les noves incorporacions currículum i titulació , però no es comproven les referències.

Proposta de millora

Caldria fer una comprovació de les referències i llocs de treball anteriors, si ni han.

(1) **Categoria:** menor

Control ISO 27001	(2) **Nivell 3**
7.1 Abans de la contractació. 7.1.1 Investigació d'antecedents.	

No conformitat	*Auditor*	*Data*
NC3	D.Butxaca	13/03/2019

Descripció

S'haurien protegir els mitjans que contenen informació contra accés no autoritzat, mal ús o corrupció durant el transport fora dels límits físics de l'organització.

Proposta de millora

Caldria encriptar la informació de equips que es treguin fora de la fundació.

(1) **Categoria :** menor

Control ISO 27001	(2) **Nivell 4**
8.3.3 Suports físics en trànsit..	

No conformitat	*Auditor*	*Data*
NC4	A.Rodriguez	11/03/2019

Descripció

S'ha millorat la gestió de les baixes però falta un control i registre dels canvis en els privilegis d'usuari sobretot en els rols assignats en el programa savac.
Aquests canvis son habituals.

Proposta de millora

Cal protocol·litzar la tasca i portar un registre

(1) **Categoria:** menor

Control ISO 27001	(2) **Nivell 3**
9.2.5 Revisió dels drets d'accés dels usuaris. 9.2.6 Retirada o adaptació dels drets d'accés	

No conformitat	*Auditor*	*Data*
NC5	D.Butxaca	12/03/2019

Descripció

Esta contractada la ,missatgeria office 365, aquesta aplicació es segura però no realitza copies de seguretat dels missatges,

Proposta de millora

cal contractar un tercer producte com per exemple Altharo

(1) **Categoria:** menor

Control ISO 27001	(2) **Nivell 4**
13.2.3 Missatgeria electrònica.	

No conformitat	*Auditor*	*Data*
NC6	D.Butxaca	9/03/2019

Descripció

Els mòbils que utilitzen las cuidadores a domicili de la Residencia, no tenen les xarxes wifi inhabilitades per l'aplicació MDM.

Proposta de millora

Cal preveure aquesta situació en que es podrien connectar a xarxes de terces insegures i inhabilitar aquesta funció.

(1) **Categoria:** menor

Control ISO 27001	(2) **Nivell 4**
14.1.2 Seguretat de les comunicacions en serveis accessibles per xarxes públiques	

No conformitat	*Auditor*	*Data*
NC7	D.Butxaca	4/03/2019

Descripció

No es porta un registre dels canvis en els paquets de programari.

Proposta de millora

S'hauria de impedir la modificació dels paquets de programari, restringint-se a l'imprescindible i tots els canvis haurien de ser estrictament controlats.

(1) **Categoria:** menor

Control ISO 27001	(2) **Nivell 3**
14.2.4 Restriccions als canvis en els paquets de programari.	

No conformitat	*Auditor*	*Data*
NC8	A.Rodriguez	4/03/2019

Descripció

Falta una política de gestió de controls criptogràfics.

Proposta de millora

Els controls criptogràfics s'han d'utilitzar d'acord amb tots els contractes, lleis i regulacions pertinents
Caldria definir una política.

(1) **Categoria:** menor

Control ISO 27001	(2) **Nivell 2**
18.1.5 Regulació dels controls criptogràfics	

(1) Categoria

Les no conformitats menors indiquen una discrepància respecte a un punt d'un domini de la norma. Les majors en canvi indicarien una falta de incompliment d'un domini complet

(2) Classificació importància constatacions

Nivell :

5-Critic : Resoldre immediatament que sigui possible
4-Important: Resoldre en quant e sigui possible
3-Moderadament important : No ha de ser ignorat ni assumit, s'ha de resoldre
2-Lleugerament important: Es pot esperar a la propera re configuració planificada
però no ha de ser ignorat ni assumit
1-A títol informatiu : es recomana que es gestioni no que s'ignori o s'assumeixi

Annexa 17: Auditoria UOC2019MMS, revisió documentació

Chec list documentació revisada per domini

A.5 POLÍTIQUES DE SEGURETAT DE LA INFORMACIÓ

A.5.1 DIRECTRIUS DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ

Objectiu: Proporcionar orientació i suport a la gestió de la seguretat de la informació d'acord amb els requisits del negoci, les lleis i normativa pertinents.

- ✓ Polítiques i objectius de seguretat de la informació

A.6 ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ

A.6.1 ORGANITZACIÓ INTERNA

Objectiu: Establir un marc de gestió per iniciar i controlar la implementació i operació de la seguretat de la informació dins de l'organització

- ✓ Marc normatiu de la Fundació
- ✓ Gestió de rols i responsabilitats de la seguretat

A.6.2 ELS DISPOSITIUS MÒBILS I EL TELETREBALL

Objectiu: Garantir la seguretat en el teletreball i en l'ús de dispositius mòbils.

- ✓ Política sobre dispositius mòbils i tele-treball
- ✓ llistat de persones amb accés remot i VPN

A.7 SEGURETAT RELATIVA ALS RECURSOS HUMANS

A.7.1 ABANS DE L'OCUPACIÓ

Objectiu: Per assegurar que els empleats i contractistes entenguin les seves responsabilitats i són adequats per a les funcions per a les que es consideren.

- ✓ Registres de capacitació, habilitats, experiència i qualificacions

A.7.2 DURANT L'OCUPACIÓ

Objectiu: Assegurar que els empleats i contractistes coneguin i compleixin amb les seves responsabilitats en seguretat de la informació

- ✓ Registre de accions formatives de seguretat

A.7.3 FINALITZACIÓ DE L'OCUPACIÓ O CANVI EN EL LLOC DE TREBALL

Objectiu: Protegir els interessos de l'organització com a part del procés de canvi o finalització de l'ocupació.

- ✓ Registre de altes i baixes d'usuaris

A.8 GESTIÓ D'ACTIUS

A.8.1 RESPONSABILITAT SOBRE ELS ACTIUS

Objectiu: Identificar els actius de l'organització i definir les responsabilitats de protecció adequades.

- ✓ Inventari d'actius i responsables
- ✓ Política d'Ús acceptable dels actius
- ✓

A.8.2 Classificació de la informació

Objectiu: Assegurar que la informació rebi un nivell adequat de protecció d'acord amb la seva importància per a l'organització.

- ✓ Política de classificació de la informació

A.8.3 Manipulació dels suports

Objectiu: Evitar la revelació, modificació, eliminació o destrucció no autoritzades de la informació emmagatzemada en suports

- ✓ *Política d'eliminació i destrucció de suports*

A.9 Control d'accés

A.9.1 Requisits de negoci per al control d'accés

Objectiu: Limitar l'accés als recursos de tractament de la informació i a la informació.

- ✓ Política de control d'accés
- ✓ Inventari de suports i
- ✓ registre d'entrada i sortida de suports

A.9.2 Gestió d'accés d'usuari

Objectiu: Garantir l'accés d'usuaris autoritzats i evitar l'accés no autoritzat als sistemes i serveis.

- ✓ Política de claus
- ✓ Relació d'usuaris, accessos autoritzats i funcions

A.9.3 Responsabilitats de l'usuari

Objectiu: Perquè els usuaris es facin responsables de salvaguardar la informació d'accés

- ✓ Revisió de resultat d'indicadors de contrasenyes segures

A.9.4 Control d'accés a sistemes i aplicacions

Objectiu: Prevenir l'accés no autoritzat als sistemes i aplicacions.

- ✓ Revisió de accés mensuals a savac i aegerus
- ✓ Revisió de accions de penalització

A.10 Criptografia

A.10.1 Controls criptogràfics

Objectiu: Garantir un ús adequat i eficaç de la criptografia per protegir la confidencialitat, autenticitat i / o integritat de la informació.

- ✓ procediments de criptografia

- ✓ revisio

A.11 SEGURETAT FÍSICA I DE L'ENTORN

A.11.1 ÀREES SEGURES

Objectiu: Prevenir l'accés físic no autoritzat, els danys i interferència a la informació de l'organització i als recursos de tractament de la informació.

- ✓ Procediment per a treball en àrees segures

A.11.2 SEGURETAT DELS EQUIPS

Objectiu: Evitar la pèrdua, dany, robatori o el compromís dels actius i la interrupció de les operacions de la organització.

- ✓ Política de pantalla i escriptori net
- ✓ Política de prevenció robatori equips
- ✓ Pòlisses d'assegurança

A.12 SEGURETAT DE LES OPERACIONS

A.12.1 PROCEDIMENTS I RESPONSABILITATS OPERACIONALS

Objectiu: Assegurar el funcionament correcte i segur de les instal·lacions de tractament de la informació.

- ✓ Procediments operatius per a gestió de TI
- ✓ Política de gestió de canvi

A.12.2 PROTECCIÓ CONTRA EL PROGRAMARI MALICIÓS (MALWARE)

Objectiu: Assegurar que els recursos de tractament d'informació i la informació estan protegits contra el malware.

- ✓ Procediment instal·lació anti-virus i anti malware

A.12.3 CÒPIES DE SEGURETAT

Objectiu: Evitar la pèrdua de dades

- ✓ Plans de contingència

A.12.4 REGISTRES I SUPERVISIÓ

Objectiu: Registrar esdeveniments i generar evidències.

- ✓ Política de creació de còpies de seguretat

A.12.5 CONTROL DEL PROGRAMARI EN EXPLOTACIÓ

Objectiu: Assegurar la integritat del programari en explotació.

A.12.7 CONSIDERACIONS SOBRE L'AUDITORIA DE SISTEMES D'INFORMACIÓ

Objectiu: Minimitzar l'impacte de les activitats d'auditoria en els sistemes operatius

- ✓ Procediment per auditoria interna

A.13 SEGURETAT DE LES COMUNICACIONS

A.13.1 GESTIÓ DE LA SEGURETAT DE LES XARXES

Objectiu: Assegurar la protecció de la informació en les xarxes i els recursos de tractament de la informació.

- ✓ Normativa de VLAN
- ✓ politiques de Firewalls

A.13.2 INTERCANVI D'INFORMACIÓ

Objectiu: Mantenir la seguretat de la informació que es transfereix dins d'una organització i amb qualsevol entitat externa.

- ✓ Política de transferència de la informació

A.14 ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ

A.14.1 REQUISITS DE SEGURETAT EN ELS SISTEMES D'INFORMACIÓ

Objectiu: Garantir que la seguretat de la informació sigui part integral dels sistemes d'informació a través de tot el cicle de vida. Això també inclou els requisits per als sistemes d'informació que proporcionen els serveis a través de xarxes públiques.

- ✓ Política d'adquisicions de TI

A.14.2 SEGURETAT EN EL DESENVOLUPAMENT I EN ELS PROCESSOS DE SUPORT

Objectiu: Garantir la seguretat de la informació que s'ha dissenyat i implementat en el cicle de vida de
desenvolupament dels sistemes d'informació.

- ✓ Principis d'enginyeria per a sistema segur

A.14.3 DADES DE PROVA

Objectiu: Assegurar la protecció de les dades de prova

- ✓ Procediment de anonimitzacio de dades de prova

A.15 RELACIÓ AMB PROVEÏDORS

A.15.1 SEGURETAT EN LES RELACIONS AMB PROVEÏDORS

Objectiu: Assegurar la protecció dels actius de l'organització que siguin accessibles als proveïdors.

- ✓ Política de seguretat per a proveïdors
- ✓ Política de encarregats de tractament

A.15.2 GESTIÓ DE LA PROVISIÓ DE SERVEIS DEL PROVEÏDOR

Objectiu: Mantenir un nivell acordat de seguretat i de provisió de serveis en línia amb acords amb proveïdors

- ✓ Llista de encarregats de tractament i revisió contractes SLA
- ✓ Contractes de manteniment i serveis

A.16 Gestió d'incidents de seguretat de la informació

A.16.1 Gestió d'incidents de seguretat de la informació i millores

Objectiu: Assegurar un enfocament coherent i eficaç per a la gestió d'incidents de seguretat de la informació, inclosa la comunicació d'esdeveniments de seguretat i debilitats

- ✓ Metodologia d'avaluació i tractament de riscos
- ✓ Declaració d'aplicabilitat
- ✓ Pla de tractament del risc
- ✓ Procediment per a gestió d'incidents

A.17 Aspectes de seguretat de la informació per a la gestió de la continuïtat de negoci

A.17.1 Continuïtat de la seguretat de la informació

Objectiu: La continuïtat de la seguretat de la informació ha de formar part dels sistemes de gestió de la continuïtat de negoci de l'organització.

- ✓ Procediments de la continuïtat del negoci
- ✓ Anàlisi de l'impacta en el negoci.
- ✓ Pla de manteniment i revisió

A.17.2 Redundàncies.

Objectiu: Assegurar la disponibilitat dels recursos de tractament de la informació.

- ✓ procediment de replicació de VM entre CPd1-CPd2
- ✓ Disseny físic i lògic dels sistemes d'informació

A.18 Compliment

A.18.1 Compliment dels requisits legals i contractuals

Objectiu: Evitar incompliments de les obligacions legals, estatutàries, reglamentàries o contractuals relatives a la seguretat de la informació o dels requisits de seguretat.

- ✓ Informe sobre avaluació i tractament de riscos
- ✓ Requisits legals, normatius i contractuals

A.18.2 Revisions de la seguretat de la informació

Objectiu: Garantir que la seguretat de la informació s'implementa i opera d'acord amb les polítiques i procediments de l'organització.

- ✓ Procediment per a control de documents
- ✓ Controls per a gestió de registres
- ✓ Resultats d'accions correctives
- ✓ Registres sobre activitats dels usuaris, excepcions i esdeveniments de
- ✓ seguretat
- ✓ Actes del comitè de seguretat

Annexa 18

Annexa A (normatiu) ISO 27001: 2017

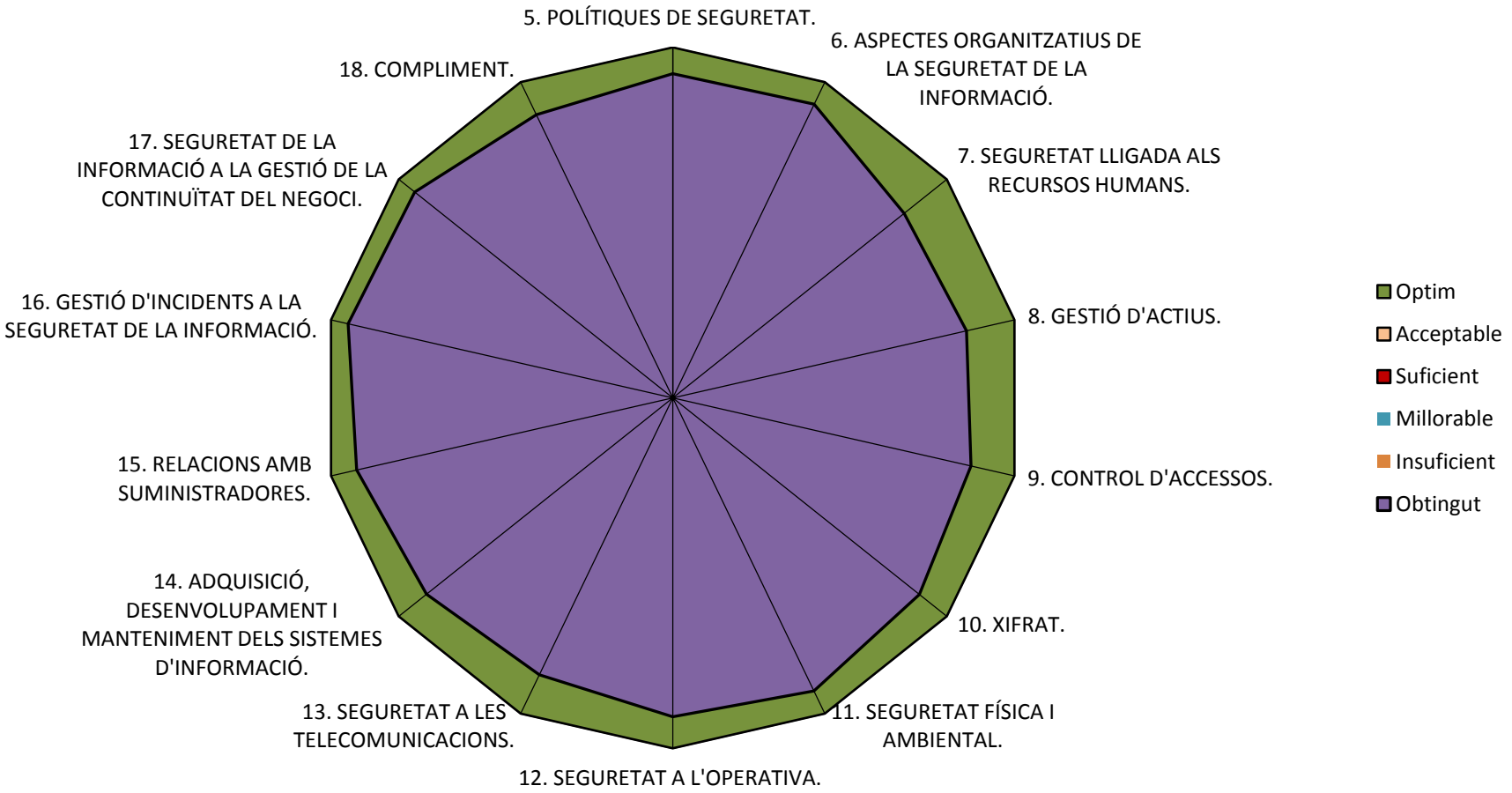
Objectius de control i controls de referència

Valors obtinguts una vegada implementats els projectes

ID	Nivell
5	Optimitzat
4	Gestionat
3	Definit
2	Repetible
1	Inicial
0	Inexistent

	Valor
5. POLÍTIQUES DE SEGURETAT.	4,625
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	4,65
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS.	4,222
8. GESTIÓ D'ACTIUS.	4,299
9. CONTROL D'ACCESSOS.	4,365
10. XIFRAT.	4,5
11. SEGURETAT FÍSICA I AMBIENTAL.	4,642
12. SEGURETAT A L'OPERATIVA.	4,55
13. SEGURETAT A LES TELECOMUNICACIONS.	4,386
14. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ.	4,493
15. RELACIONS AMB SUMINISTRADORES.	4,625
16. GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	4,75
17. SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.	4,709
18. COMPLIMENT.	4,484

Anàlisis GAP actual



Comparativa amb els valors anteriors

	Valor	Actual	Millora
5. POLÍTIQUES DE SEGURETAT.	**2,5**	**4,6**	2,1
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	**3,45**	**4,6**	1,15
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS.	**3,55**	**4,2**	0,65
8. GESTIÓ D'ACTIUS.	**2,05**	**4,3**	2,25
9. CONTROL D'ACCESSOS.	**3,5**	**4,3**	0,8
10. XIFRAT.	**2,5**	**4,5**	2
11. SEGURETAT FÍSICA I AMBIENTAL.	**4,3**	**4,6**	0,3
12. SEGURETAT A L'OPERATIVA.	**3,7**	**4,5**	0,8
13. SEGURETAT A LES TELECOMUNICACIONS.	**3,4**	**4,4**	1
14. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ.	**3,25**	**4,5**	1,25
15. RELACIONS AMB SUMINISTRADORES.	**3,625**	**4,6**	0,975
16. GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	**4,75**	**4,75**	0,0
17. SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.	**4,05**	**4,7**	0,65
18. COMPLIMENT.	**4,15**	**4,5**	0,35

A continuación es presenten els resultats de l'anàlisi diferencial inicial en forma de taula de la implantació dels controls de la ISO/IEC 27002:2013.

Anàlisi de Compliment inicial	Inicial	Posterior	Dif.
control Implantació			
5. POLÍTIQUES DE SEGURETAT.	**50,0**	**92,5**	**42,5**
5.1 Directrius de la Direcció en seguretat de la informació.	50,0	92,5	42,5
5.1.1 Conjunt de polítiques per a la seguretat de la informació.	90,0	90,0	0,0
5.1.2 Revisió de les polítiques per a la seguretat de la informació.	10,0	95,0	85,0
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	**69,0**	**93,0**	**24,0**
6.1 Organització interna.	88,0	96,0	8,0
6.1.1 Assignació de responsabilitats per a la segur. de la informació.	95,0	95,0	0,0
6.1.2 Segregació de tasques.	95,0	95,0	0,0
6.1.3 Contacte amb les autoritats.	100,0	100,0	0,0
6.1.4 Contacte amb grups d'interès especial.	50,0	90,0	40,0
6.1.5 Seguretat de la informació en la gestió de projectes.	100,0	100,0	0,0
6.2 Dispositius per a mobilitat i teletreball.	50,0	90,0	40,0
6.2.1 Política d'ús de dispositius per a mobilitat.	50,0	90,0	40,0
6.2.2 Teletreball.	50,0	90,0	40,0
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS.	**71,1**	**84,4**	**13,3**
7.1 Abans de la contractació.	70,0	70,0	0,0
7.1.1 Investigació d'antecedents.	50,0	50,0	0,0
7.1.2 Condicions de contractació.	90,0	90,0	0,0
7.2 Durant la contractació.	93,3	93,3	0,0
7.2.1 Responsabilitats de gestió.	95,0	95,0	0,0
7.2.2 Conscienciació, educació i capacitació en segur. de la informac.	95,0	95,0	0,0
7.2.3 Procés disciplinari.	90,0	90,0	0,0
7.3 Cessament o canvi de lloc de treball.	50,0	90,0	40,0
7.3.1 Cessament o canvi de lloc de treball.	50,0	90,0	40,0
8. GESTIÓ D'ACTIUS.	41,1	86,0	44,9
8.1 Responsabilitat sobre els actius. 8	50,0	91,3	41,3
8.1.1 Inventari d'actius.	90,0	95,0	5,0
8.1.2 Propietat dels actius.	50,0	90,0	40,0
8.1.3 Ús acceptable dels actius.	50,0	90,0	40,0
8.1.4 Devolució d'actius.	10,0	90,0	80,0
8.2 Classificació de la informació.	50,0	90,0	40,0
8.2.1 Directrius de classificació.	50,0	90,0	40,0
8.2.2 Etiquetatge i manipulat de la informació.	50,0	90,0	40,0
8.2.3 Manipulació d'actius.	50,0	90,0	40,0
8.3 Maneig dels suports d'emmagatzematge.	23,3	76,7	53,3
8.3.1 Gestió de suports extraïbles.	10,0	90,0	80,0
8.3.2 Eliminació de suports.	50,0	90,0	40,0
8.3.3 Suports físics en trànsit.	10,0	50,0	40,0
9. CONTROL D'ACCESSOS.	69,7	87,3	17,6
9.1 Requisits de negoci per al control d'accessos.	90,0	92,5	2,5
9.1.1 Política de control d'accessos.	90,0	90,0	0,0

9.1.2 Control d'accés a les xarxes i serveis associats.	90,0	95,0	5,0
9.2 Gestió d'accés d'usuari.	56,7	76,7	20,0
9.2.1 Gestió d'altes / baixes en el registre d'usuaris.	90,0	90,0	0,0
9.2.2 Gestió dels drets d'accés assignats a usuaris.	90,0	90,0	0,0
9.2.3 Gestió dels drets d'accés amb privilegis especials.	90,0	90,0	0,0
9.2.4 Gestió d'informació confidencial d'autenticació d'usuaris.	50,0	90,0	40,0
9.2.5 Revisió dels drets d'accés dels usuaris.	10,0	50,0	40,0
9.2.6 Retirada o adaptació dels drets d'accés	10,0	50,0	40,0
9.3 Responsabilitats de l'usuari.	50,0	90,0	40,0
9.3.1 Ús d'informació confidencial per a l'autenticació.	50,0	90,0	40,0
9.4 Control d'accés a sistemes i aplicacions.	82,0	90,0	8,0
9.4.1 Restricció de l'accés a la informació.	90,0	90,0	0,0
9.4.2 Procediments segurs d'inici de sessió.	90,0	90,0	0,0
9.4.3 Gestió de contrasenyes d'usuari.	90,0	90,0	0,0
9.4.4 Ús d'eines d'administració de sistemes.	90,0	90,0	0,0
9.4.5 Control d'accés al codi font dels programes.	50,0	90,0	40,0
10. XIFRAT.	50,0	**90,0**	**40,0**
10.1 Controls criptogràfics.	50,0	90,0	40,0
10.1.1 Política d'ús dels controls criptogràfics.	50,0	90,0	40,0
10.1.2 Gestió de claus.	50,0	90,0	40,0
11. SEGURETAT FÍSICA I AMBIENTAL.	86,2	92,8	6,7
11.1 Àrees segures.	94,0	94,0	0,0
11.1.1 perímetre de seguretat física.	95,0	95,0	0,0
11.1.2 Controls físics d'entrada.	95,0	95,0	0,0
11.1.3 Seguretat d'oficines, despatxos i recursos.	90,0	90,0	0,0
11.1.4 Protecció contra les amenaces externes i ambientals.	95,0	95,0	0,0
11.1.5 El treball en àrees segures.	95,0	95,0	0,0
11.1.6 Àrees d'accés públic, càrrega i descàrrega.	90,0	90,0	0,0
11.2 Seguretat dels equips.	78,3	91,7	13,3
11.2.1 Emplaçament i protecció d'equips.	95,0	95,0	0,0
11.2.2 Instal·lacions de subministrament.	90,0	90,0	0,0
11.2.3 Seguretat del cablejat.	90,0	90,0	0,0
11.2.4 Manteniment dels equips.	50,0	90,0	40,0
11.2.5 Sortida d'actius fora de les dependències de l'empresa.	50,0	90,0	40,0
11.2.6 Seguretat dels equips i actius fora de les instal·lacions.	90,0	90,0	0,0
11.2.7 Reutilització o retirada segura de dispositius d'emmagatzematge.	50,0	90,0	40,0
11.2.8 Equip informàtic d'usuari desatès.	95,0	95,0	0,0
11.2.9 Política de lloc de treball buidat i bloqueig de pantalla.	95,0	95,0	0,0
12. SEGURETAT A L'OPERATIVA.	74,4	91,0	16,7
12.1 Responsabilitats i procediments d'operació.	60,0	90,0	30,0
12.1.1 Documentació de procediments d'operació.	50,0	90,0	40,0
12.1.2 Gestió de canvis.	50,0	90,0	40,0
12.1.3 Gestió de capacitats.	50,0	90,0	40,0
12.1.4 Separació d'entorns de desenvolupament, prova i producció.	90,0	90,0	0,0
12.2 Protecció contra codi maliciós.	50,0	90,0	40,0
12.2.1 Controls contra el codi maliciós.	50,0	90,0	40,0
12.3 Còpies de seguretat.	95,0	95,0	0,0

12.3.1 Còpies de seguretat de la informació.	95,0	95,0	0,0
12.4 Registre d'activitat i supervisió.	81,3	91,3	10,0
12.4.1 Registre i gestió d'esdeveniments d'activitat.	50,0	90,0	40,0
12.4.2 Protecció dels registres d'informació.	90,0	90,0	0,0
12.4.3 Registres d'activitat de l'administrador i operador del sistema.	90,0	90,0	0,0
12.4.4 Sincronització de rellotges.	95,0	95,0	0,0
12.5 Control del programari en explotació.	90,0	90,0	0,0
12.5.1 Instal·lació del programari en sistemes en producció.	90,0	90,0	0,0
12.6 Gestió de la vulnerabilitat tècnica.	70,0	90,0	20,0
12.6.1 Gestió de les vulnerabilitats tècniques.	50,0	90,0	40,0
12.6.2 Restriccions en la instal·lació de programari.	90,0	90,0	0,0
12.7 Consideracions de les auditories dels sistemes d'informació.	95,0	95,0	0,0
12.7.1 Controls d'auditoria de	95,0	95,0	0,0
13. SEGURETAT A LES TELECOMUNICACIONS.	67,7	87,7	20,0
13.1 Gestió de la seguretat en les xarxes.	51,7	91,7	40,0
13.1.1 Controls de xarxa.	10,0	90,0	80,0
13.1.2 Mecanismes de seguretat associats a serveis en xarxa.	50,0	90,0	40,0
13.1.3 Segregació de xarxes.	95,0	95,0	0,0
13.2 Intercanvi d'informació amb parts externes.	83,8	83,8	0,0
13.2.1 Polítiques i procediments d'intercanvi d'informació.	95,0	95,0	0,0
13.2.2 Acords d'intercanvi.	95,0	95,0	0,0
13.2.3 Missatgeria electrònica.	50,0	50,0	0,0
13.2.4 Acords de confidencialitat i secret.	95,0	95,0	0,0
14. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ.	65,6	89,9	24,3
14.1 Requisits de seguretat dels sistemes d'informació.	51,7	78,3	26,7
14.1.1 Anàlisi i especificació dels requisits de seguretat.	50,0	90,0	40,0
14.1.2 Seguretat de les comunicacions en serveis accessibles per xarxes públiques.	10,0	50,0	40,0
14.1.3 Protecció de les transaccions per xarxes telemàtiques.	95,0	95,0	0,0
14.2 Seguretat en els processos de desenvolupament i suport.	50,0	96,3	46,3
14.2.1 Política de desenvolupament segur de programari.	50,0	90,0	40,0
14.2.2 Procediments de control de canvis en els sistemes.	50,0	90,0	40,0
14.2.3 Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu.	50,0	90,0	40,0
14.2.4 Restriccions als canvis en els paquets de programari.	50,0	50,0	0,0
14.2.5 Ús de principis d'enginyeria en protecció de sistemes.	50,0	90,0	40,0
14.2.6 Seguretat en entorns de desenvolupament.	50,0	90,0	40,0
14.2.7 Externalització del desenvolupament de programari.	40,0	90,0	50,0
14.2.8 Proves de funcionalitat durant el desenvolupament dels sistemes.	50,0	90,0	40,0
14.2.9 Proves d'acceptació.	50,0	90,0	40,0
14.3 Dades de prova.	95,0	95,0	0,0
14.3.1 Protecció de les dades utilitzades en proves.	95,0	95,0	0,0
15. RELACIONS AMB SUMINISTRADORES.	72,5	92,5	20,0
15.1 Seguretat de la informació en les relacions amb subministradors.	95,0	95,0	0,0
15.1.1 Política de seguretat de la informació per subministradors.	95,0	95,0	0,0
15.1.2 Tractament del risc dins d'acords de subministradors.	95,0	95,0	0,0
15.1.3 Cadena de subministrament en tecnologies de la informació i comunicacions.	95,0	95,0	0,0

15.2 Gestió de la prestació del servei per subministradors.	50,0	90,0	40,0
15.2.1 Supervisió i revisió dels serveis prestats per tercers.	50,0	90,0	40,0
15.2.2 Gestió de canvis en els serveis prestats per tercers.	50,0	90,0	40,0
16. GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	95,0	95,0	0,0
16.1 Gestió d'incidents de seguretat de la informació i millores.	95,0	95,0	0,0
16.1.1 Responsabilitats i procediments.	95,0	95,0	0,0
16.1.2 Notificació dels esdeveniments de seguretat de la informació.	95,0	95,0	0,0
16.1.3 Notificació de punts febles de la seguretat.	95,0	95,0	0,0
16.1.4 Valoració d'esdeveniments de seguretat de la informació i presa de decisions.	95,0	95,0	0,0
16.1.5 Resposta als incidents de seguretat.	95,0	95,0	0,0
16.1.6 Aprenentatge dels incidents de seguretat de la informació.	95,0	95,0	0,0
16.1.7 Recull d'evidències.	95,0	95,0	0,0
17. SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.	80,8	94,2	13,3
17.1 Continuïtat de la seguretat de la informació.	66,7	93,3	26,7
17.1.1 Planificació de la continuïtat de la seguretat de la informació.	95,0	95,0	0,0
17.1.2 Implantació de la continuïtat de la seguretat de la informació.	95,0	95,0	0,0
17.1.3 Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	10,0	90,0	80,0
17.2 Redundàncies.	95,0	95,0	0,0
17.2.1 Disponibilitat d'instal·lacions per al processament de la informació.	95,0	95,0	0,0
18. COMPLIMENT.	83,0	89,7	6,7
18.1 Compliment dels requisits legals i contractuals.	86,0	86,0	0,0
18.1.1 Identificació de la legislació aplicable.	95,0	95,0	0,0
18.1.2 Drets de propietat intel·lectual (DPI).	95,0	95,0	0,0
18.1.3 Protecció dels registres de l'organització.	95,0	95,0	0,0
18.1.4 Protecció de dades i privacitat de la informació personal.	95,0	95,0	0,0
18.1.5 Regulació dels controls criptogràfics.	50,0	50,0	0,0
18.2 Revisions de la seguretat de la informació.	80,0	93,3	13,3
18.2.1 Revisió independent de la seguretat de la informació.	95,0	95,0	0,0
18.2.2 Compliment de les polítiques i normes de seguretat.	95,0	95,0	0,0
18.2.3 Comprovació del compliment	50,0	90,0	40,0