Pla Director de Seguretat de la UNIF

Nom Estudiant: ALBERT PINTU PLA

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

Nom Consultor: ARSENIO TORTAJADA GALLEGO

Data Lliurament: 04/01/2017

FITXA DEL TREBALL FINAL

Títol del treball:	Pla Director de Seguretat de la UNIF
Nom de l'autor:	***Albert Pintu Pla***
Nom del consultor:	***Arsenio Tortajada Gallego***
Data de lliurament (mm/aaaa):	*01/2017*
Àrea del Treball Final:	***SGSI***
Titulació:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball:

L'objectiu del projecte és l'elaboració d'un Pla Director de Seguretat per una universitat d'àmbit públic, que anomenarem de manera fictícia UNIF (Universitat Fictícia). La informació continguda en aquest projecte ha estat manipulada per no reflectir la situació real de cap universitat en concret, tot i que en tot moment s'ha intentat que aquesta informació conservi un grau elevat de veracitat.

El Pla de Seguretat s'emmarca segons la norma ISO 27001:2013 i establirà les especificacions d'implementació, supervisió, gestió i millora d'un Sistema Gestor de Seguretat de la Informació (SGSI). En el projecte es realitza un anàlisi de la situació actual i es defineixen unes propostes per pal·liar les deficiències trobades. L'objectiu, per tant, és trobar aquelles propostes que millorin la seguretat de l'organització i establir unes prioritats per la implementació de les mateixes. Per acomplir aquests objectius s'ha recorregut a metodologies com Magerit.

Abstract:

The aim of the project is to develop of a Security Master Plan for a public sphere university that we call fictitiously UNIF. The information contained on this project has been manipulated to not reflect the real situation of any particular university, but keeping a high degree of information accuracy.

The Safety Plan is conducted according ISO 27001: 2013. The ISO establishes the specifications for implement, monitor, manage and improve a Management System Information Security (ISMS). The project does an analysis of the current situation and defines proposals to remedy the deficiencies found. The aim, therefore, is to find proposals that will improve the security of

the organization and establish priorities for implementing it. To accomplish these objectives Magerit metodology is used.

Paraules clau:

SGSI, ISO 27000, pla director de seguretat.

Índex

Index de figures

1. Introducció

1.1 Context i justificació del Treball

Aquest document constitueix la memòria tècnica corresponent al Treball Fi del Màster Interuniversitari de les Tecnologies de la informació i comunicacions (MISTIC) cursat a la UOC.

El Treball Fi de Màster (TFM) consisteix en l'elaboració d'un Pla Director de Seguretat basant-nos en la norma ISO 27001, versió 2013. En aquest treball ens basarem sobre una organització real, una Universitat, però a efectes de confidencialitat durant tot el document l'organització serà anomenada com a "UNIF – Universitat Fictícia". Així mateix alguns aspectes tècnics i dades proporcionades poden ser omeses o canviats amb dades fictícies a afectes de mantenir aquesta confidencialitat.

Moltes organitzacions i empreses consideren la informació com un dels seus valors més importants. La disponibilitat, integritat, confidencialitat i autenticitat de la informació, juntament amb els processos i elements que la tracten esdevenen essencials i indispensables pel funcionament d'aquestes organitzacions. En aquest context i lligat a una creixent conscienciació de la seguretat de la informació, juntament amb un marc legal que cal complir, promou la realització d'accions al respecte per part d'empreses i organitzacions.

Com a resposta a aquesta situació la UNIF ha creat un equip de Seguretat, el qual tindrà com uns dels objectius inicials desenvolupar un Pla de Director de Seguretat.

1.2 Objectius del Treball

Els objectius específics d'aquest treball seran:

- Garantir el compliment de la legislació vigent.
- Identificar els riscos de l'organització.
- Crear accions de conscienciació al personal respecte a la seguretat de la informació.
- Implicar les àrees i departaments més rellevants.
- Garantir la Integritat, Confidencialitat i Disponibilitat de la informació.
- Establir, implementar i mantenir un Sistema de Gestió de la Seguretat de la informació.
- Establir cicles de millora contínua en referència a la gestió de la seguretat.

1.3 Enfocament i mètode seguit

Aquest projecte es desenvoluparà segons les següents fases:

- Fase 1: Situació actual: Contextualització, objectius i anàlisis diferencial

La Introducció al Projecte. Enfoc i selecció de l'empresa que serà objecte d'estudi. Definició dels objectius del Pla Director de Seguretat i Anàlisis diferencial de l'empresa amb respecte a la ISO/IEC 27001+ISO/IEC 27002.

- Fase 2: Sistema de Gestió Documental

Elaboració de la Política de Seguretat. Declaració de l'aplicabilitat i documentació del SGSI.

- Fase 3: Anàlisis de riscos

Elaboració d'una metodologia d'anàlisis de riscos: Identificació i valoració dels actius, amenaces, vulnerabilitats, càlcul del risc, nivell de risc acceptable i risc residual.

- Fase 4: Proposta de Projectes

Avaluació de projectes que ha de portar a terme la Organització per alinear-se amb els objectius plantejats al Pla Director. Quantificació econòmica i temporal d'aquests.

- Fase 5: Auditoria de Compliment de la ISO/IEC 27002:2013

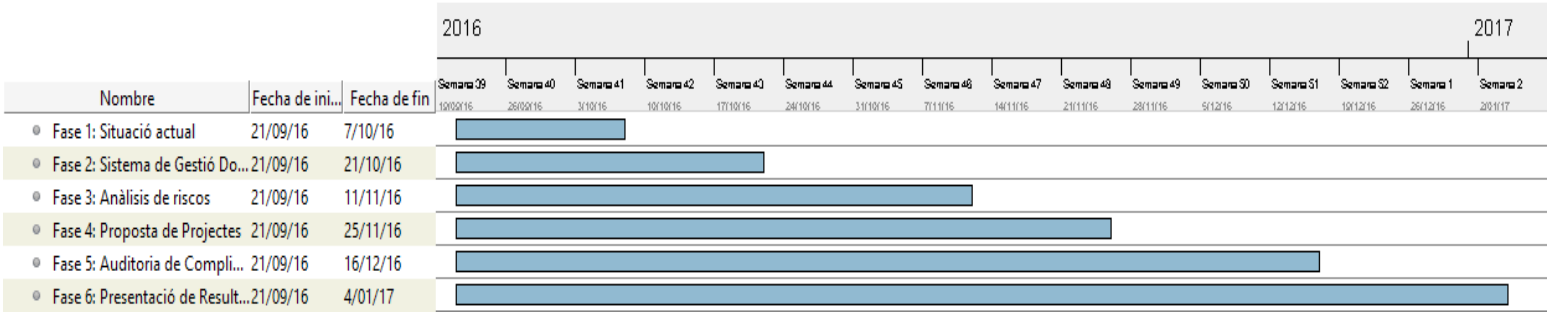
Avaluació de controls, maduresa i nivell de compliment.

- Fase 6: Presentació de Resultats i entrega de Informes

Consolidació dels resultats obtinguts durant el procés d'anàlisis. Realització dels informes i presentació executiva a Direcció. Entrega del projecte final.

1.4 Planificació del Treball

DIAGRAMA DE GANTT:



2. Contextualització

En aquest projecte es realitzarà un Pla Director de Seguretat per una Universitat Pública que anomenarem de forma fictícia UNIF. Totes les dades aquí presentades poden estar manipulades per tal de preservar la confidencialitat i anonimat de la mateixa.

A continuació s'indicaran els detalls més rellevants de l'organització que permetran comprendre l'enfocament del Pla Director de Seguretat que es desenvoluparà.

2.1 Descripció de l'empresa

La Universitat dona servei a una comunitat aproximadament de 15000 persones dels quals 11000 són estudiants de graus i màsters, 1000 doctorands, 2000 docents i 1000 treballadors. Aquests tenen com a centre de treball tres Campus universitaris ubicats a la mateixa àrea metropolitana i diferents edificis.

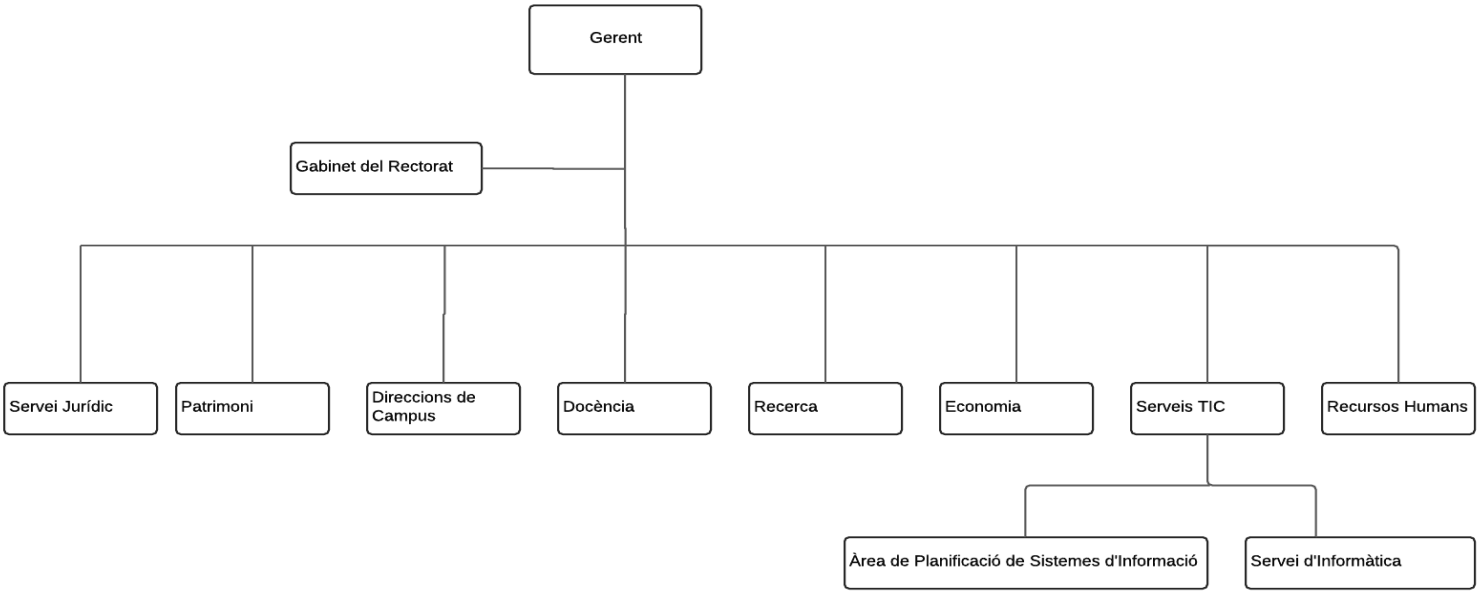
2.2 Estructura Organitzativa

Existeix una dualitat organitzativa: la acadèmica i l'administrativa.

L'estructura acadèmica la componen:

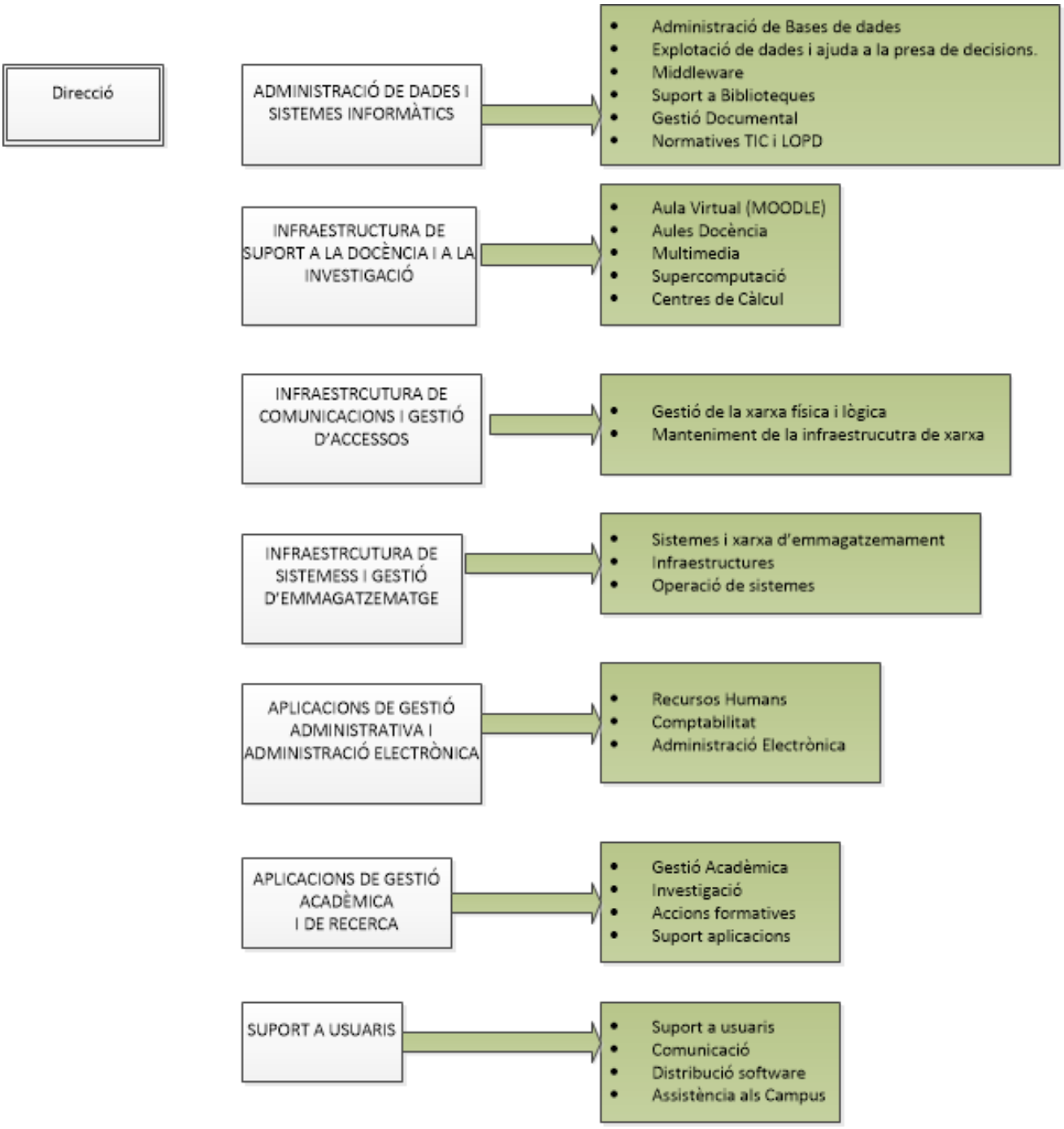
- Unitats acadèmiques (secretaries)
- Facultats i centres
- Departaments
- Centres adscrits
- Centres de recerca i Instituts universitaris
- Càtedres

L'estructura administrativa disposa d'una estructura jeràrquica més precisa:



Nota: S'ha simplificat l'estructura per representar una visió més generalista de la mateixa però igualment efectiva per l'objecte d'aquest estudi.

A continuació detallem l'estructura funcional del Servei d'Informàtica on es detallen les diferents unitats que depenen de la direcció d'informàtica juntament amb les seves funcionalitats:



2.3 Localització

La Universitat disposa de 3 Campus.

Cada Campus consta del següent número d'edificis:

- Campus A: 5
- Campus B: 5
- Campus C: 2

El 80% de la comunitat té com a lloc de treball o estudi els Campus A i B. Tots els Campus disposen d'estructures per la docència (aules, tallers, biblioteques, etc) així com d'espais per el professorat i els investigadors (oficines, laboratoris, etc).

2.4 Infraestructures IT

A continuació s'enumeren breument les tecnologies utilitzades en els serveis centrals, els quals seran l'objecte principal d'estudi. Per la complexitat que representa en aquest estudi no es considerarà la infraestructura IT pròpia de grups de recerca o entitats amb infraestructura IT pròpia.

Sistemes Operatius:

- SUSE Sles
- Ubuntu
- Windows Server 2012
- Solaris

Servidors d'aplicacions*:

- Apache/Tomcat
- Weblogic

Bases de Dades:

- Oracle
- Mysql
- SQL Server

Serveis de directori[1]:

- Active Directory
- Novell eDirectory
- Gestor d'identitats - CAS

Serveis d'emmagatzematge:

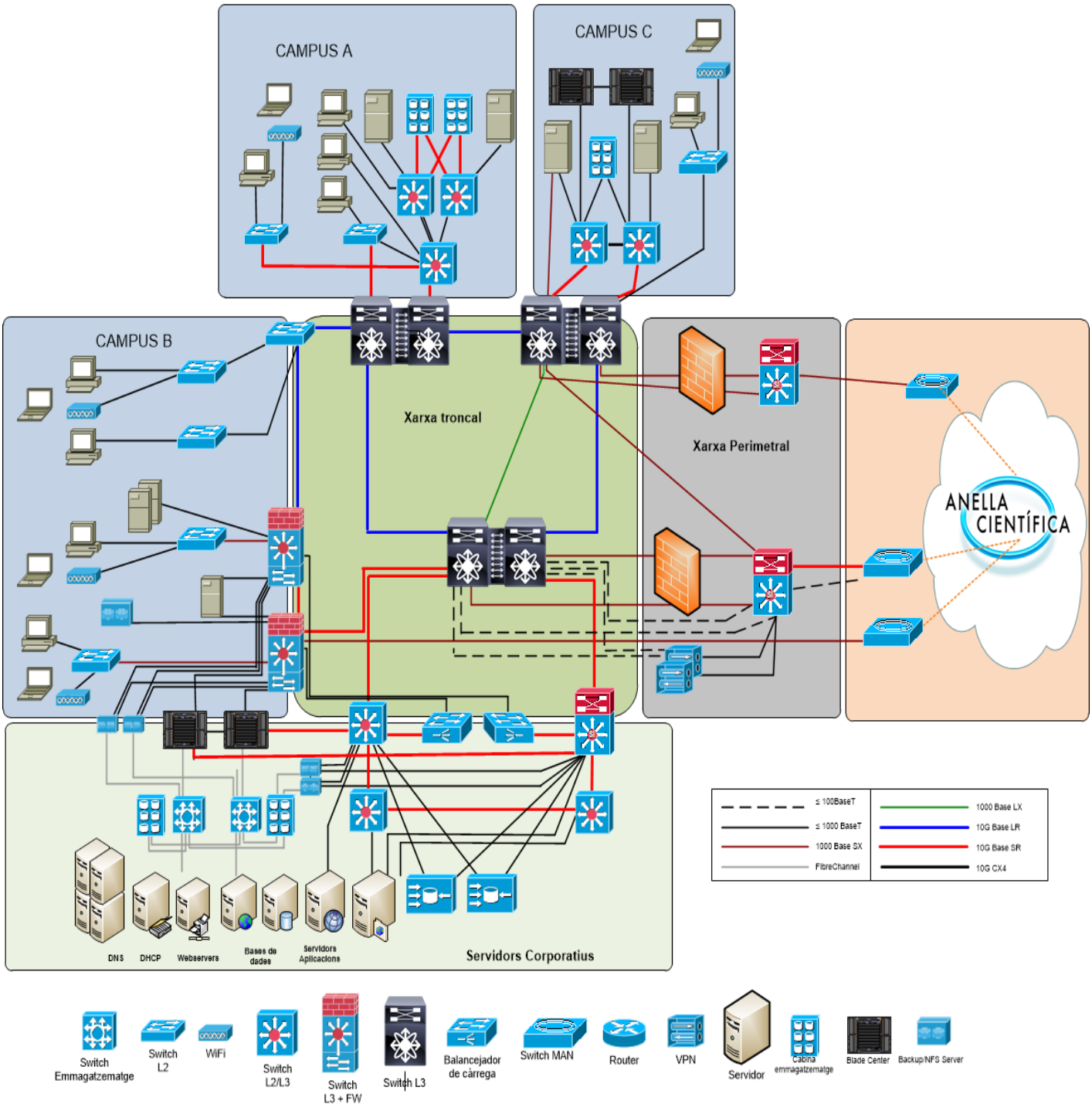
- NetApp
- EMC

Xarxes:

- Connexió amb fibra entre edificis i Campus i connexió a través de l'anella científica
- Wifi: Controladores, AP's
- Tallafocs perimetrals
- Proxy d'accés a Internet
- Configuració de xarxes a través de VLAN's. Existeixen diferents VLAN's segons l'edifici o ubicació i/o dispositius (impressores, workstations, aules, dispositius)

1 Actualment s'està realitzant la migració de Novell eDirectory cap a Microsoft Active Directory

Esquema global de l'estructura de xarxa:



Centres de càlcul: Es disposa d'un CPD ubicat a cada campus.

CPD A, B i C:

3. Objectius del Pla Director

Aquest Pla Director de Seguretat pretén avaluar l'estat actual de les àrees IT de l'organització donades les creixents necessitats de crear un equip de seguretat. Aquestes accions es duran a terme ja sigui mitjançant la creació d'un departament específic o amb la creació d'un equip transversal. La primera part d'aquest projecte és doncs conèixer i veure l'estat en el qual la organització es troba.

A partir d'aquest Pla Director es visualitzaran les necessitats de l'organització permetent potenciar millores immediates i d'altres a mitjà-llarg termini. Paral·lelament s'identificaran els recursos necessaris per dur-les a terme.

Aquelles àrees que ja es trobin immerses en projectes d'implementació requeriran procediments de control i execució que tindran per objectiu revisar les mesures existents i assegurar-se del seu correcte funcionament. Aquests controls seran periòdics al llarg del procés d'implementació de les corresponents mesures .

La metodologia empleada en el procés de millora continua del sistema de gestió es basarà en PDCA (Planificar, Fer, Verificar i Actual) .

En aquest Pla Director es seguiran les normes de la família ISO 27000, és a dir, les ISO/IEC 27001 i ISO/IEC 27002, publicades per la International Organization for Standardization[2] (ISO).

4. Abast

L'abast d'aquest document serà realitzar un Pla de director de Seguretat dels serveis IT, on s'inclourà tota la infraestructura de l'àrea IT dels serveis centrals. Entendrem com a serveis centrals aquells serveis i processos que donen servei de forma homogènia a tota la comunitat, per exemple, serveis d'autenticació, aplicacions corporatives, etc.

Aquest treball no inclourà aquelles àrees IT específiques ja sigui de facultats, departaments o grups d'investigació que tinguin la seva pròpia infraestructura o que treballin de forma independent.

En aquest document no s'abordarà la seguretat física dels edificis però si que es farà incís en l'accés als centres de càlcul.

2ISO- Organització no governamental que es compon per diferents representants d'organismes de normalització de més de 150 països. La seva funció és l'elaboració d'estàndards i normes internacionals per molts camps de la indústria i el comerç.

5. Anàlisi compliment inicial

Es detalla a continuació l'anàlisi diferencial de les mesures de seguretat. Aquest anàlisis diferencial es realitza respecte a als 114 controls o mesures preventives , organitzats en 14 àrees i 35 objectius de control de la i ISO/IEC 27002. Això ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

5.1 Nivells de Maduresa

El Model de Maduresa de Capacitats o CMM (Capability Maturity Model) analitza el nivell de maduresa de les organitzacions mitjançant l'avaluació dels seus processos. En aquest sentit, distingeix cinc "nivells de maduresa" (com mostrem a sota), de manera que es considera que una organització que tingui institucionalitzades totes les pràctiques incloses en un nivell i els seus inferiors ha arribat a aquest nivell de maduresa.

La següent taula, basada en el model de maduresa de capacitat (CMM), ens mostrarà aquesta valoració:

	Descripció
Inexistent	Carència completa de qualsevol procés que reconeguem.
Inicial	Les organitzacions en aquest nivell no disposen d'un ambient estable per al desenvolupament i manteniment de programari. Encara que s'utilitzin tècniques correctes d'enginyeria, els esforços es veuen minats per falta de planificació. L'èxit dels projectes es basa la majoria de les vegades en l'esforç personal, encara que sovint es produeixen fracassos i gairebé sempre retards i sobre costos. El resultat dels projectes és impredictible.
Repetible	En aquest nivell les organitzacions disposen d'unes pràctiques institucionalitzades de gestió de projectes, hi ha unes mètriques bàsiques i un raonable seguiment de la qualitat. La relació amb subcontractistes i clients està gestionada sistemàticament.
Definit	A més d'una bona gestió de projectes, a aquest nivell les organitzacions disposen de correctes procediments de coordinació entre grups, formació del personal, tècniques d'enginyeria més detallades i un nivell més avançat de mètriques en els processos. S'implementen tècniques de revisió per parells (exàmens per homòlegs).
Gestionat	Es caracteritza perquè les organitzacions disposen d'un conjunt de mètriques significatives de qualitat i productivitat, que s'usen de manera sistemàtica per a la presa de decisions i la gestió de riscos. El programari resultant és d'alta qualitat.
Optimitzat	L'organització completa està bolcada en la millora contínua dels processos. Es fa ús intensiu de les mètriques i es gestiona el procés d'innovació.

Font: Guia metodològica de projectes per a l'anàlisi i millora de processos, Secretaria de Funció Pública i Modernització de l'Administració, Generalitat de Catalunya.

5.2 Metodologia

Per determinar el nivell de maduresa de cada un dels controls i clàusules es realitzen entrevistes amb els responsables dels sistemes d'informació, administradors dels sistemes d'informació i de la infraestructura tecnològica juntament amb responsables de direcció. La informació obtinguda es complementa amb la revisió dels processos i procediments que formen part dels processos més comuns a l'organització.

Taula de ponderació utilitzada:

	Efectivitat
Inexistent	0%
Inicial	10%
Repetible	50%
Definit	90%
Gestionat	95%
Optimitzat	100%

5.3 Resultats

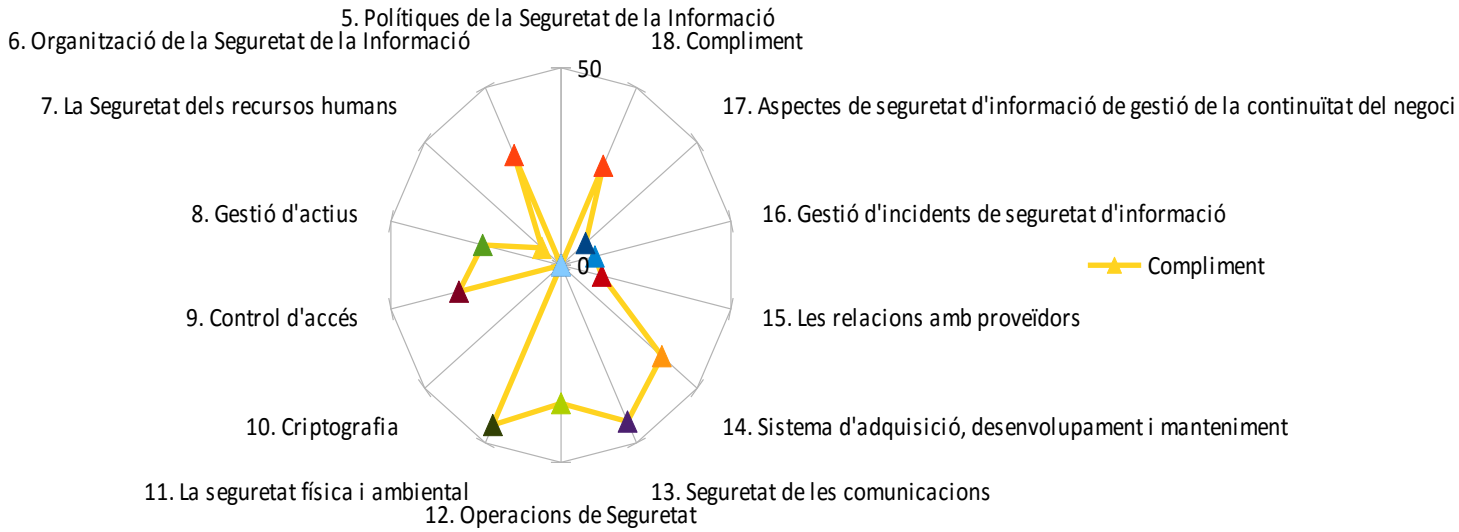
S'adjunta a l'ANNEX I l'anàlisi diferencial detallat.

La següent taula mostra el resum de l'anàlisi diferencial:

CONTROLS	**SITUACIÓ ACTUAL**
5. Polítiques de la Seguretat de la Informació	0%
6. Organització de la Seguretat de la Informació	31%
7. La Seguretat dels recursos humans	7%
8. Gestió d'actius	23%
9. Control d'accés	30%

10. Criptografia	0%
11. La seguretat física i ambiental	45%
12. Operacions de Seguretat	35%
13. Seguretat de les comunicacions	44%
14. Sistema d'adquisició, desenvolupament i manteniment	37%
15. Les relacions amb proveïdors	12%
16. Gestió d'incidents de seguretat d'informació	10%
17. Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	9%
18. Compliment	28%

La següent gràfica il·lustra el grau de maduresa global:



Respecte a les àrees on més deficiències es detecten podem extrapolar-ne:

5. Polítiques de la Seguretat de la Informació: Evidentment en aquest punt la principal problemàtica és la carència en si mateix d'una política de seguretat definida.

7. La Seguretat dels recursos humans: No es realitza un seguiment durant la vida laboral de l'empleat i la gestió dels seu desenvolupament dins l'empresa no té una supervisió clara en aspectes de seguretat.

10. Criptografia: Si bé cada departament o unitat intenta securitzar el seu entorn no hi ha una política comuna i sovint aquesta tasca esdevé una decisió personal de l'administrador o tècnic final de cada recurs.

15. Les relacions amb proveïdors: En aquest punt, tot i que si està treballant, tampoc existeix una política comuna, i o no s'apliquen clàusules que facin referència a la seguretat o s'apliquen diferents criteris.

16. Gestió d'incidents de seguretat d'informació: Es troba a faltar la mancança de canals de comunicació efectius, referents, i finalment un grup visible de seguretat.

17. Aspectes de seguretat d'informació de gestió de la continuïtat del negoci: S'està treballant en un model mixt d'infraestructura externa/interna que permetrà assegurar els aspectes de la continuïtat del negoci.

6. Esquema Documental

6.1 Introducció

La política de seguretat és la insígnia principal d'un sistema de gestió de la seguretat, donat que constitueix el primer nivell de la jerarquia en seguretat de la informació.

La Política de Seguretat s'adjunta a l'ANNEX II

6.2 Objectius

Els objectius per definir d'aquesta política són establir les directrius en seguretat de la informació, respectant la legislació aplicable juntament amb els objectius i compromisos de la UNIF.

Específicament els objectius són:

- Prendre les accions necessàries perquè el Sistema de Gestió de Seguretat de la Informació millori contínuament.
- Gestionar els incidents de seguretat de la informació de tal manera que l'impacte a l'organització es minimitzi en cas que es materialitzi un risc.

- Crear consciència als empleats, directius, proveïdors i personal extern respecte a la Seguretat de la Informació.
- Protegir la confidencialitat, integritat, i disponibilitat de la informació que emmagatzemin, processin, transportin, generin o accedeixin els actius d'informació de l'organització.

6.3 Procediment d'Auditories Internes

El SGSI serà auditat amb una periodicitat anual. Les auditories internes seran executades per un tercer idoni tenint en compte que la UNIF no compta amb un àrea d'auditoria interna. Els tercers contractats seran designats per el Comitè de Seguretat TI prèviament superant una fase de concurs i selecció. Hauran de complir amb els següents requisits:

- Han de garantir la independència respecte el procés o treball auditat.
- Títol professional com a Enginyer de Sistemes, Electrònic, Informàtic, Telecomunicacions o afins.
- Tres anys d'experiència en auditories de sistemes.
- Haver participat en almenys 3 auditories de Sistemes de Gestió de Seguretat pel que fa a la norma ISO 27001 en el rol d'auditor o auditor principal.
- Demostrar experiència en consultoria, assessoria i/o auditoria en temes relacionats amb Seguretat de la Informació.

6.3.1 Procediment d'execució d'Auditories Internes

El pla d'auditoria haurà d'executar-se d'acord amb el procediment presentat en l'ANNEX III d'aquest document.

6.3.2 Formats /Plantilles

El pla d'auditoria haurà de desenvolupar-se d'acord els formats de les plantilles presentades en l'ANNEX III d'aquest document.

6.4 Gestió Indicadors de Seguretat

Per mesurar l'estat de Seguretat de la Informació, l'eficàcia i la seva eficiència utilitzarem els indicadors de seguretat. Es descriuran amb la següent taula:

Àrea de Control a la que fa referència	
Objectiu	Descripció de l'objectiu de la mesura.
Definició	Explicació sobre l'objectiu de la mesura.
Responsable	Persona sobre qui recau la responsabilitat de proporcionar el resultat de la mesura.
Freqüència	Cada quant s'ha de recollir la mesura. Pot ser variable, existint una freqüència inicial i una posterior.
Formula de la mesura	Descripció concreta de la fórmula aplicada per a obtenir la mesura.
Descripció dels valors	Explicació detallada sobre com s'obtenen aquests valors.
Valor Objectiu	Són els valors objectiu i llindar que té per objectiu l'organització.

Podem distingir diferents tipologies d'indicadors:

- De Gestió: Número de treballadors, pressupost dedicat a la plantilla de personal, hores de formació impartides, etc.
- D'Operació: Estadístiques del tallafocs, nombre de deteccions d'un IDS, nombre d'infeccions de virus o malware a les workstations, etc.
- D'Entorn: Legislació aplicable, temps d'aplicació de solucions de seguretat des de que es detecta una vulnerabilitat i climatologia, obres, o instal·lacions elèctriques que puguin afectar els equips.

A l'ANNEX IV en descrivim alguns.

6.5 Procediment de revisió per direcció

El SGSI de la UNIF estableix la realització d'una revisió anual per part de la direcció. Aquesta revisió té una periodicitat anual i te com a objectiu assegurar l'adequació i efectivitat dels propòsits del SGSI. Consta dels següents passos:

- El responsable de seguretat realitza una recopilació de la informació necessària, entre ella:
    - Resultats de les auditories internes.
    - Mètriques de compliment del SGSI.
    - Resultats de les actuacions aplicades a partir de les no conformitats.
    - Resum dels incidents de seguretat.
    - Actualització de la gestió i tractament de riscos.
- Realització de l'informe d'entrada. Es facilita una plantilla a l'.
- Convocatòria de reunió per la revisió anual on s'analitza la informació aportada per determinar accions de millora.
- Generació d'informe de sortida on es recullen les conclusions i decisions preses. Es facilita una plantilla a l'.

6.6 Metodologia d'anàlisi de riscos.

A l'ANNEX V es troba la metodologia seguida per el càlcul de l'anàlisi de riscos seguint el mètode Magerit.

6.7 Declaració d'aplicabilitat.

L'objectiu principal de la declaració d'aplicabilitat és especificar quin dels 114 controls o mesures preventives són els que s'implementarà en l'organització.

Es pot llegir el document de declaració d'aplicabilitat a l'ANNEX VI

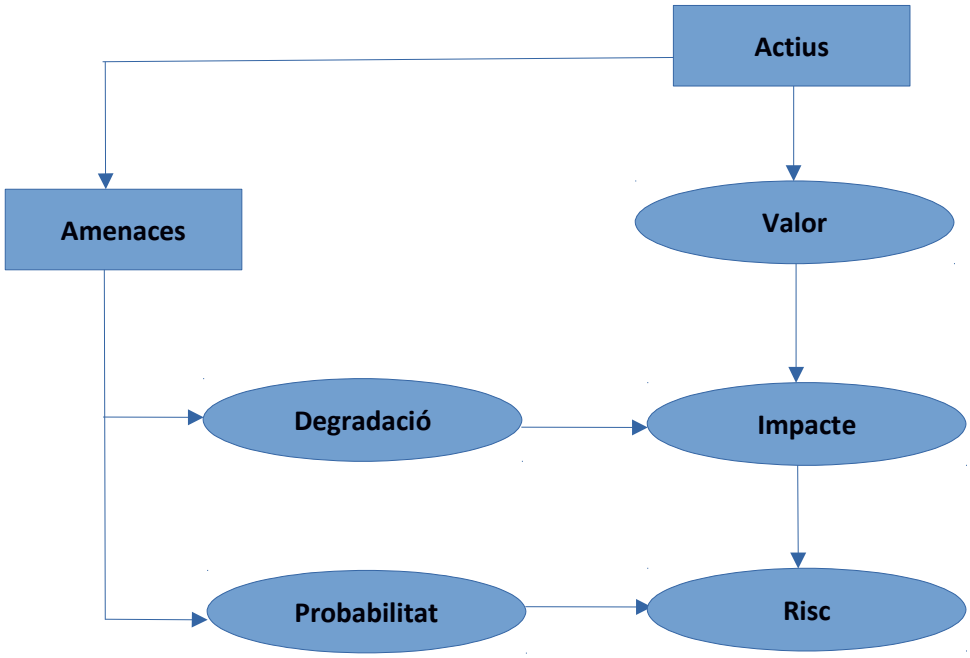
7. Anàlisis de riscos

7.1 Introducció

Es basarà l'execució de l'anàlisi de riscos en la metodologia proposada a MAGERIT v3. Es troben més detalls en el capítol 6.

L'anàlisi de riscos és una aproximació metòdica per determinar el risc seguint uns passos pautats:

- Determinar els actius rellevants per l'organització, la seva interrelació, i el seu valor en cas de degradació i el seu perjudici associat.
- Determinar a quines amenaces estan exposats els actius.
- Determinar quines salvaguardes estan disponibles i la seva eficàcia.
- Estimar l'impacte, definit com el perjudici sobre l'actiu derivat de la materialització de l'amenaça.
- Estimar el risc, definit com l'impacte ponderat amb la tassa de freqüència (o expectativa de materialització) de l'amenaça.



7.2 Inventari d'actius

Els actius considerats en aquest anàlisi seran aquells elements del Sistema de la Informació necessaris per a l'activitat del negoci.

Els actius s'han classificat segons les seves característiques, seguint l'agrupació proposada per Magerit:

- Instal·lacions: Són tots els elements que disposa l'organització i que necessita per assegurar el correcte funcionament de la resta d'elements. Per exemple: sistemes d'aire condicionat, cablejat de dades, corrent elèctric.
- Maquinari: Són tots els elements de hardware que s'utilitzen en l'organització. Per exemple: pc's, servidors, portàtils, tabletes, telèfons mòbils i fixes, impressores, etc.
- Aplicacions: Són tots els elements de programari que s'utilitzen en l'organització. Per exemple: aplicacions de gestió, aplicacions de suport, sistemes operatius, etc.
- Dades: Són els elements que contenen la informació que permet a una organització prestar els seus serveis. Per exemple: Bases de Dades, copies de seguretat, etc.
- Xarxa: Són tots els elements que transporten dades d'un lloc a un altre. Per exemple: Routers, Switch, WiFi, Mòbils, etc.
- Serveis: Són els elements que satisfan i proveeixen necessitats als usuaris.
- Equipament auxiliar: Són els elements que estan relacionats directament amb el tractament de dades. Per exemple: caixes ignifugues, SAI's, sistemes de refrigeració, etc.
- Personal: Són les persones, des del punt de vista de rols o perfils que intervenen en el desenvolupament de les activitats de l'organització. Per exemple: El responsable de seguretat, administrador del sistema/xarxa, personal d'administració, etc.

Índex d'elements de la Taula d'inventari:

Instal·lacions	
Codi	**Actiu**
I.1	Centre de Càlcul 1 (CPD)
I.2	Centre de Càlcul 2 (CPD)
I.3	Centre de Càlcul 3 (CPD)
I.4	Arxiu.
I.5	RITI 1. (Recinte d'instal·lacions de Telecomunicacions)
I.6	RITI 2.
I.7	RITI 3.

Maquinari (Hardware)	
Codi	**Actiu**
H.1	Workstations
H.2	Portàtils
H.3	Tablets
H.4	Mòbils
H.5	Impressores
H.6	Routers
H.7	Switchs
H.8	Tallafocs
H.9	Balancejadors de càrrega
H.10	Proxys
H.11	Cabines de disc
H.12	Cluster VMWARE
H.13	Cluster ORACLE
H.14	Centraleta telefonia IP
H.15	SIEM
H.16	IDS/IPS
H.17	Controladores WiFi + Acces Points

Aplicacions (Software)	
Codi	**Actiu**
A.1	Sistemes operatius clients (Windows, Linux, MacOS)

A.2	Windows Server 2012R2
A.3	SUSE Enterprise
A.4	Solaris
A.5	Apache Tomcat
A.6	Weblogic
A.7	Antivirus
A.8	Offimàtica
A.9	Oracle Database
A.10	Software gestió backups (Coomvault, VEEM)
A.11	Software Gestió Acadèmic
A.12	OpenCMS/Liferay Portal/Intranet
A.13	Novell
A.14	VMWARE

Dades	
Codi	**Actiu**
D.1	Backup
D.2	Dades RRHH
D.3	Documentum
D.4	Dades alumnes
D.5	Correu i eines de col·laboració (al núvol)

Xarxa	
Codi	**Actiu**

X.1	Connexions primàries fibra amb anella científica
X.2	Connexió secundària fibra amb anella científica
X.3	Routers/Switch
X.4	Xarxa wifi: Controladores + Acces Points

Serveis	
Codi	**Actiu**
S.1	Impressió
S.2	Web
S.3	Correu + eines col·laboratives
S.4	Formació

Equipament auxiliar	
Codi	**Actiu**
AUX.1	Armaris racks CPDs
AUX.2	Sistema climàtic CPD
AUX.3	Sistemes d'alimentació continua i secundària
AUX.4	Cablejat elèctric
AUX.5	Cablejat xarxa
AUX.6	Sistema antiincendis

Personal	
Codi	**Actiu**
P.1	Responsable del departament TI

P.2	Responsable de seguretat
P.3	Desenvolupadors
P.4	Personal de sistemes i comunicacions

7.3 Valoració dels actius

La valoració d'actius consistirà en assignar una valoració econòmica a tots els actius que es pretenen analitzar.

Es defineixen uns rangs econòmics segons la valoració dels actius:

Valoració	Valor
Molt Alt	**300.000€**
Alt	**175.000€**
Mitjà	**75.000€**
Baix	**30.000€**
Molt Baix	**10.000€**
Menyspreable	**3.000€**

Per realitzar la valoració es tindrà en consideració:

- Valor de reposició.

  Valor que té per a l'organització reposar l'actiu en cas que es pèrdua o que sigui impossible la seva utilització.

- Valor de configuració.

  Temps necessari des que s'adquireix un nou actiu fins que es pot utilitzar per a la mateixa funció que desenvolupava l'anterior actiu.

- Valor d'ús.

  Valor que perd l'organització durant el temps que no pot utilitzar l'actiu per a la funció que desenvolupa.

- Valor de pèrdua d'oportunitat.

Valor que perd potencialment l'organització pel fet de no poder disposar d'aquest actiu durant un temps determinat.

A mode resum indiquem la valoració d'actius segons la seva agrupació:

Agrupació/Àmbit	Valor Quantitatiu
Instal·lacions	**500000**
Hardware	**25580000**
Aplicacions	**730000**
Dades	**350000**
Xarxa	**465000**
Serveis	**1115000**
Equipament auxiliar	**600000**
Personal	**1435000**
TOTAL	**29960000**

A l'Annex VII es detalla la valoració d'actius completa.

7.4 Dimensions de seguretat

Els aspectes de seguretat més crítics els avaluem a partir de les cinc dimensions de la seguretat de la informació. Aquestes cinc dimensions són:

- Autenticitat:

  Propietat o característica consistent en que una entitat, individu o procés és qui diu ser, o bé garanteix la font origen de les dades. [UNE 71504:2008]

- Disponibilitat:

  Propietat o característica dels actius consistent en que les entitats o processos autoritzats tenen accés als actius quan ho requereixen. [UNE 71504:2008]

- Integritat:

Propietat o característica que indicaria que l'actiu d'informació no ha estat alterat de manera no autoritzada. Si la seva alteració no suposa cap preocupació, el seu valor serà menyspreable. [ISO/IEC 13335-1:2004]

- Confidencialitat:

  Propietat o característica consistent en que la informació ni es posa a disposició ni es revela a individus, entitats o processos no autoritzats. [UNE-ISO/IEC 27001:2007]

- Traçabilitat:

  Propietat o característica consistent en que les actuacions d'una entitat poden ser imputades a aquesta entitat o subjecte. [UNE 71504:2008]

L'escala sobre la que es realitzaran les valoracions seguirà el següent criteri:

Valoració	Criteri
10	**Dany molt greu a la organització**
7-9	**Dany greu a la organització**
4-6	**Dany important a la organització**
1-3	**Dany menor a la organització**
0	**Dany irrellevant a la organització**

S'adjunta a l'ANNEX VIII la taula amb l'avaluació de les dimensions de seguretat.

7.5 Anàlisi d'amenaces

En aquest punt es realitzarà una estimació de l'impacte de les possibles amenaces sobre els actius, aproximant el seu valor de probabilitat de materialització. Per cada amenaça caldrà analitzar el possible impacte en una o més de les diferents dimensions de seguretat de l'actiu.

La metodologia utilitzada categoritza les amenaces segons:

- Amenaces d'origen natural

  Per exemple: Inundacions, terratrèmols, etc.

- Amenaces d'entorn o d'origen industrial

  Incidents que solen produir-se de manera accidental, que tenen el seu origen en elements de tipus industrial. Per exemple: contaminació, fallades elèctriques.

- Errors i errors no intencionats

  Errors no intencionals causats per les persones, típicament per error o per omissió.

- Atacs intencionats

  Fallades deliberats causats per les persones, bé amb ànim de beneficiar indegudament, bé amb ànim de causar danys i perjudicis.

Un cop identificades les amenaces s'ha d'establir una valoració de la seva influència en el valor dels actius. Per fer-ho, en aquesta anàlisi s'avalua la freqüència (probable/improbable) amb la què es pot materialitzar una amenaça.

Freqüència			
Descripció	**Rang**	**Abreviatura**	**Valor**
Extremadament freqüent	Diari	EF	1
Molt freqüent	Quinzenal	MF	0,071
Freqüent	Bimensual	F	0,016
Poc freqüent	Trimestral	PF	0,005
Molt poc freqüent	Semestral	MPF	0,003
Menyspreable	Anual	M	0

7.6 Impacte Potencial

L'Impacte Potencial identifica la magnitud del dany que podria causar a l'organització el fet que arribes a succeir alguna de les amenaces.

Impacte Potencial = Valor de l'actiu x Impacte

Per realitzar aquest càlcul s'ha utilitzat:

- El valor de cada un dels actius per totes les seves dimensions, calculat en apartats anteriors.
- Impacte. Entendrem per impacte el tant per cent del valor de l'actiu que es perd en cas que hi hagi una incidència sobre aquest actiu.

Impacte potencial:

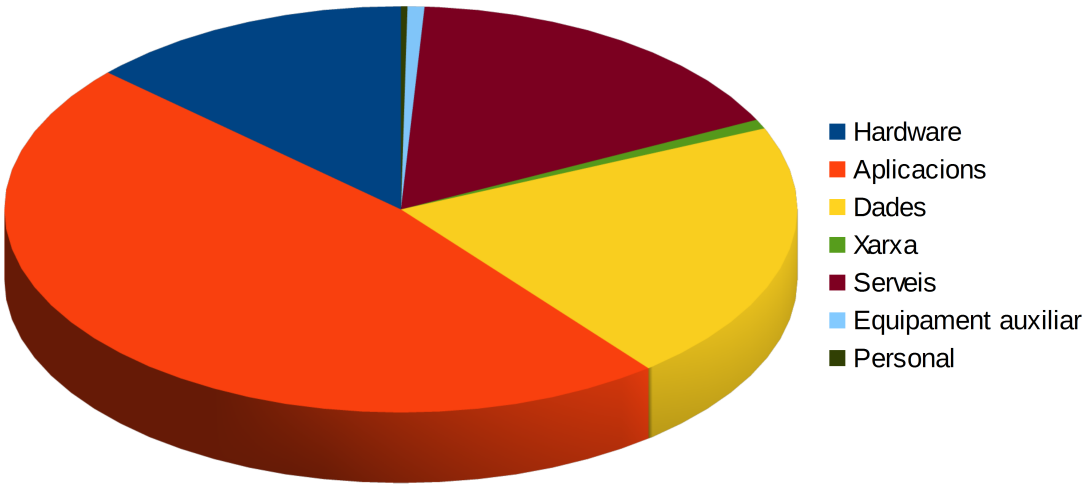
CODI	ASPECTES CRÍTICS					%IMPACTE					IMPACTE POTENCIAL				
	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
I.1	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.2	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.3	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.4	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.5	7	6	9	9	8		100	50	100		0	6	4,5	9	0
I.6	7	6	8	9	8		100	50	100		0	6	4	9	0
I.7	7	6	8	9	8		100	50	100		0	6	4	9	0
H.1	6	5	6	5	5		100	50	100		0	5	3	5	0
H.2	6	5	6	5	5		100	50	100		0	5	3	5	0
H.3	5	5	5	3	3		100	50	100		0	5	2,5	3	0
H.4	4	6	6	6	6		100	50	100		0	6	3	6	0
H.5	2	2	4	5	5		100	50	100		0	2	2	5	0
H.6	5	6	8	8	6		100	50	100		0	6	4	8	0
H.7	5	6	8	8	6		100	50	100		0	6	4	8	0
H.8	7	6	8	9	8		100	50	100		0	6	4	9	0
H.9	6	4	8	8	5		100	50	100		0	4	4	8	0
H.10	6	5	6	5	6		100	50	100		0	5	3	5	0
H.11	9	9	10	10	8		100	50	100		0	9	5	10	0
H.12	8	8	9	9	8		100	50	100		0	8	4,5	9	0
H.13	9	9	10	10	8		100	50	100		0	9	5	10	0
H.14	3	6	6	9	8		100	50	100		0	6	3	9	0
H.15	6	5	6	5	5		100	50	100		0	5	3	5	0
H.16	6	5	6	5	5		100	50	100		0	5	3	5	0
H.17	2	3	2	3	3		100	50	100		0	3	1	3	0
A.1	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.2	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.3	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.4	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.5	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.6	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.7	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.8	2	3	2	3	3	100	100	100	100		2	3	2	3	0
A.9	6	7	6	6	7	100	100	100	100		6	7	6	6	0
A.10	5	6	5	5	6	100	100	100	100		5	6	5	5	0
A.11	9	10	10	9	6	100	100	100	100		9	10	10	9	0
A.12	5	6	5	5	6	100	100	100	100		5	6	5	5	0
A.13	5	6	6	5	5	100	100	100	100		5	6	6	5	0
A.14	5	6	6	5	5	100	100	100	100		5	6	6	5	0
D.1	9	9	9	10	7	100	100	75	100		9	9	6,75	10	0
D.2	9	10	10	9	6	100	100	75	100		9	10	7,5	9	0
D.3	9	10	10	9	6	100	100	75	100		9	10	7,5	9	0
D.4	9	10	10	9	6	100	100	75	100		9	10	7,5	9	0
D.5	8	9	9	9	9	100	100	75	100		8	9	6,75	9	0
X.1	5	6	8	8	6	100	50	50	80		5	3	4	6,4	0
X.2	5	6	8	8	6	100	50	50	80		5	3	4	6,4	0
X.3	5	6	8	8	6	100	50	50	80		5	3	4	6,4	0
X.4	5	6	8	8	6	100	50	50	80		5	3	4	6,4	0
S.1	5	6	6	5	5		50	100	100		0	3	6	5	0
S.2	8	9	9	9	9	100	100	100	100	100	8	9	9	9	9
S.3	8	9	9	9	9	100	100	100	100	100	8	9	9	9	9
S.4	3	3	3	3	3				50		0	0	0	1,5	0
AUX.1				6			100	25	100		0	0	0	6	0
AUX.2				9			100	25	100		0	0	0	9	0
AUX.3				9			100	25	100		0	0	0	9	0
AUX.4				9			100	25	100		0	0	0	9	0
AUX.5				9			100	25	100		0	0	0	9	0
AUX.6				9			100	25	100		0	0	0	9	0
P.1				6			75	50	80		0	0	0	4,8	0
P.2				6			75	50	80		0	0	0	4,8	0
P.3				6			75	50	80		0	0	0	4,8	0
P.4				6			75	50	90		0	0	0	5,4	0

El segon element a calcular és el Risc Intrínsec, risc al qual l'actiu està exposat sense tenir en consideració les mesures de seguretat implantades. Per analitzar del risc intrínsec, s'ha utilitzat:

Risc Intrínsec = Impacte Potencial x Freqüència

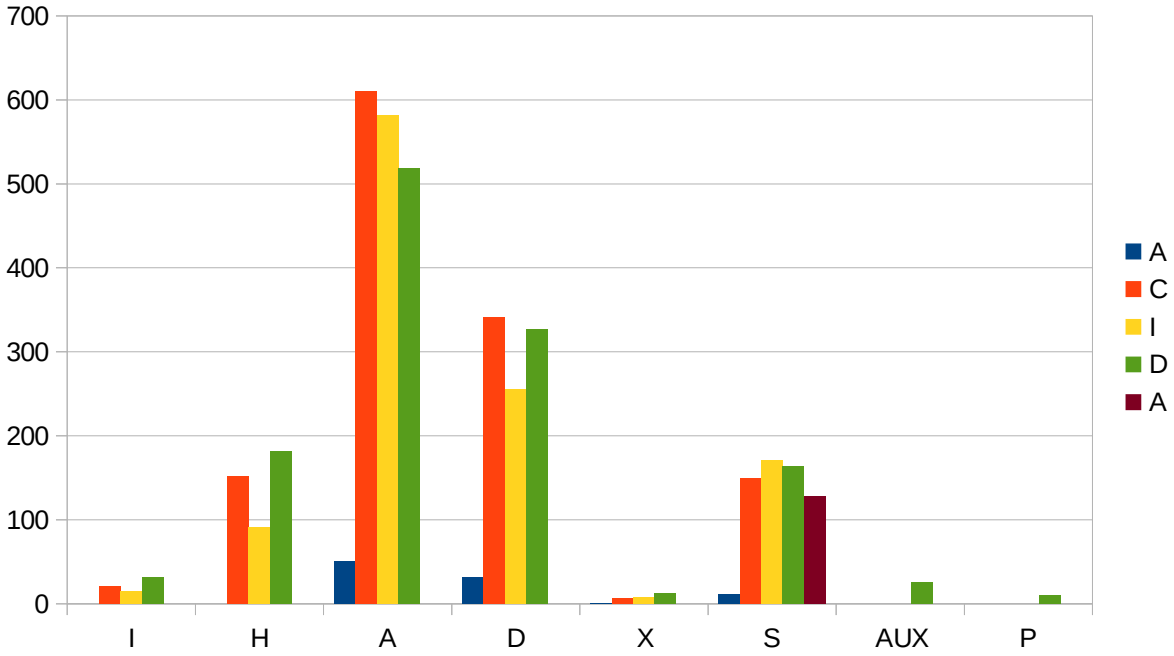
CODI	FREQ	VALOR FREQ	ASPECTES CRÍTICS					RISC				
			A	C	I	D	A	A	C	I	D	A
I.1	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.2	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.3	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.4	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.5	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.6	Baixa	0,005	0	6	4	9	0	0	3	2	4,5	0
I.7	Baixa	0,005	0	6	4	9	0	0	3	2	4,5	0
H.1	Mitja	0,016	0	5	3	5	0	0	8	4,8	8	0
H.2	Mitja	0,016	0	5	3	5	0	0	8	4,8	8	0
H.3	Mitja	0,016	0	5	2,5	3	0	0	8	4	4,8	0
H.4	Mitja	0,016	0	6	3	6	0	0	9,6	4,8	9,6	0
H.5	Mitja	0,016	0	2	2	5	0	0	3,2	3,2	8	0
H.6	Mitja	0,016	0	6	4	8	0	0	9,6	6,4	12,8	0
H.7	Mitja	0,016	0	6	4	8	0	0	9,6	6,4	12,8	0
H.8	Mitja	0,016	0	6	4	9	0	0	9,6	6,4	14,4	0
H.9	Mitja	0,016	0	4	4	8	0	0	6,4	6,4	12,8	0
H.10	Mitja	0,016	0	5	3	5	0	0	8	4,8	8	0
H.11	Mitja	0,016	0	9	5	10	0	0	14,4	8	16	0
H.12	Mitja	0,016	0	8	4,5	9	0	0	12,8	7,2	14,4	0
H.13	Mitja	0,016	0	9	5	10	0	0	14,4	8	16	0
H.14	Mitja	0,016	0	6	3	9	0	0	9,6	4,8	14,4	0
H.15	Mitja	0,016	0	5	3	5	0	0	8	4,8	8	0
H.16	Mitja	0,016	0	5	3	5	0	0	8	4,8	8	0
H.17	Mitja	0,016	0	3	1	3	0	0	4,8	1,6	4,8	0
A.1	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.2	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.3	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.4	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.5	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.6	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.7	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.8	Alta	0,071	2	3	2	3	0	1,42	21,3	14,2	21,3	0
A.9	Alta	0,071	6	7	6	6	0	4,26	49,7	42,6	42,6	0
A.10	Alta	0,071	5	6	5	5	0	3,55	42,6	35,5	35,5	0
A.11	Alta	0,071	9	10	10	9	0	6,39	71	71	63,9	0
A.12	Alta	0,071	5	6	5	5	0	3,55	42,6	35,5	35,5	0
A.13	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
A.14	Alta	0,071	5	6	6	5	0	3,55	42,6	42,6	35,5	0
D.1	Alta	0,071	9	9	6,75	10	0	6,39	63,9	47,925	71	0
D.2	Alta	0,071	9	10	7,5	9	0	6,39	71	53,25	63,9	0
D.3	Alta	0,071	9	10	7,5	9	0	6,39	71	53,25	63,9	0
D.4	Alta	0,071	9	10	7,5	9	0	6,39	71	53,25	63,9	0
D.5	Alta	0,071	8	9	6,75	9	0	5,68	63,9	47,925	63,9	0
X.1	Baixa	0,005	5	3	4	6,4	0	0,25	1,5	2	3,2	0
X.2	Baixa	0,005	5	3	4	6,4	0	0,25	1,5	2	3,2	0
X.3	Baixa	0,005	5	3	4	6,4	0	0,25	1,5	2	3,2	0
X.4	Baixa	0,005	5	3	4	6,4	0	0,25	1,5	2	3,2	0
S.1	Alta	0,071	0	3	6	5	0	0	21,3	42,6	35,5	0
S.2	Alta	0,071	8	9	9	9	9	5,68	63,9	63,9	63,9	63,9
S.3	Alta	0,071	8	9	9	9	9	5,68	63,9	63,9	63,9	63,9
S.4	Baixa	0,005	0	0	0	1,5	0	0	0	0	0,75	0
AUX.1	Baixa	0,005	0	0	0	6	0	0	0	0	3	0
AUX.2	Baixa	0,005	0	0	0	9	0	0	0	0	4,5	0
AUX.3	Baixa	0,005	0	0	0	9	0	0	0	0	4,5	0
AUX.4	Baixa	0,005	0	0	0	9	0	0	0	0	4,5	0
AUX.5	Baixa	0,005	0	0	0	9	0	0	0	0	4,5	0
AUX.6	Baixa	0,005	0	0	0	9	0	0	0	0	4,5	0
P.1	Baixa	0,005	0	0	0	4,8	0	0	0	0	2,4	0
P.2	Baixa	0,005	0	0	0	4,8	0	0	0	0	2,4	0
P.3	Baixa	0,005	0	0	0	4,8	0	0	0	0	2,4	0
P.4	Baixa	0,005	0	0	0	5,4	0	0	0	0	2,7	0

Risc Intrínsec de tots els Actius :



Vegem que les aplicacions són el grup amb un risc més elevat però proporcionalment les dades i els serveis representen el major percentatge.

Gràfica de valors acumulats:



7.7 Risc Acceptable

En aquest punt s'ha de determinar quin nivell de risc l'organització està disposada a assumir i quins factors decideix mitigar mitjançant l'aplicació de controls de seguretat.

Prèviament definim dos conceptes:

- Risc Acceptable

  És el risc que queda per sota el llindar que marca l'organització avaluada.

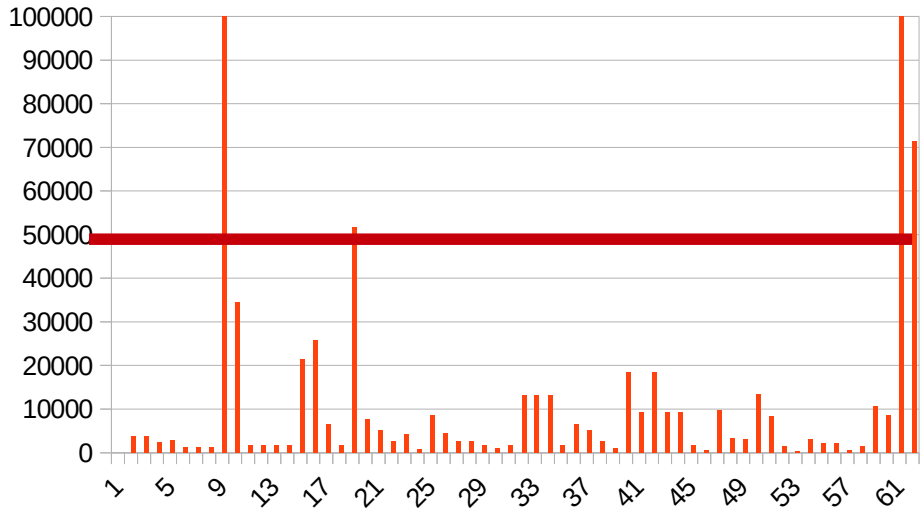
- Risc Residual

  És el risc romanent després del desplegament de les mesures de seguretat.

Per definir aquest llindar la UNIF ha de prioritzar els actius. Per fer-ho es defineixen els següents valors llindar:

Valoració	Valor Llindar
Molt Alt	**50.000€**
Alt	**20.000€**
Mitjà	**15.000€**
Baix	**3.000€**
Molt Baix	**1.000€**
Menyspreable	**500€**

Des del punt de vista d'una valoració econòmica podem observar la següent gràfica:

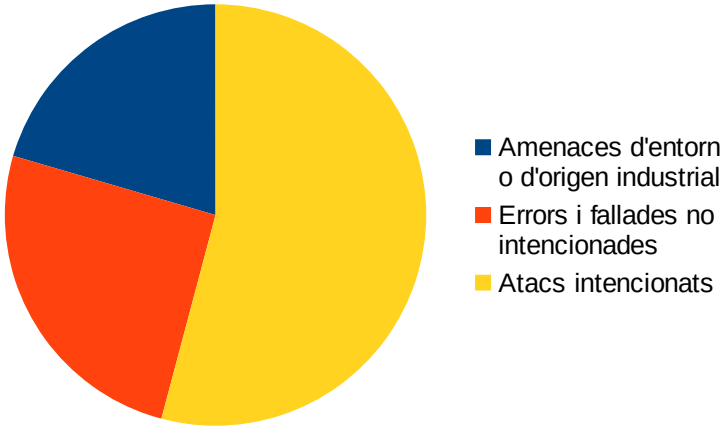


En aquest cas obtindríem que per el llindar marcat com a «Molt Alt» amb una quantificació de 50000 realment només les cabines de disc es trobarien fora d'aquest llindar.

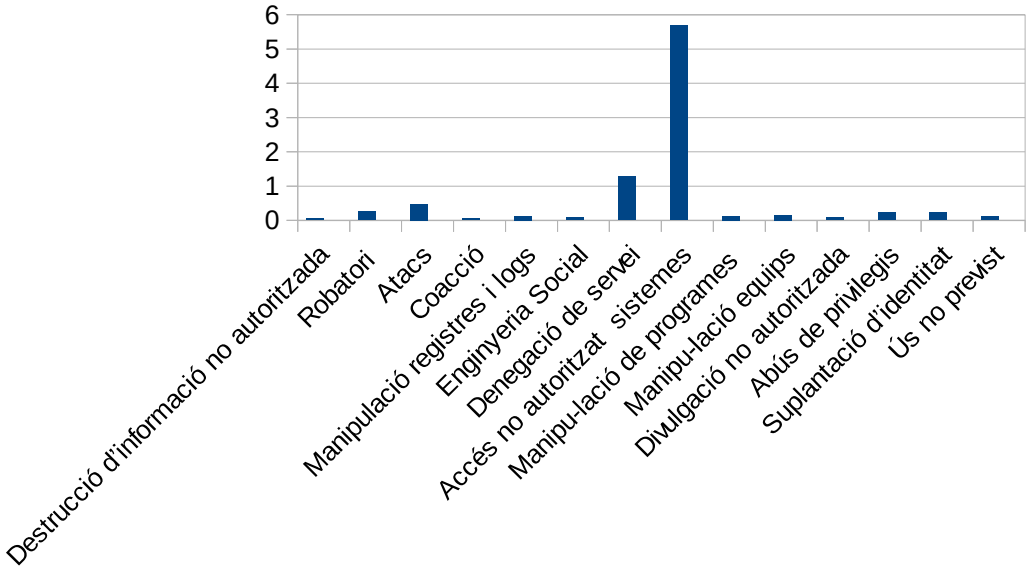
7.8 Resultats segons amenaces

En el punt anterior s'ha determinat com marcar un llindar i establir prioritats sobre els actius a través del risc intrínsec trobat.

A la següent gràfica observem la ponderació de les amenaces per categories globals a les que la organització està exposada:

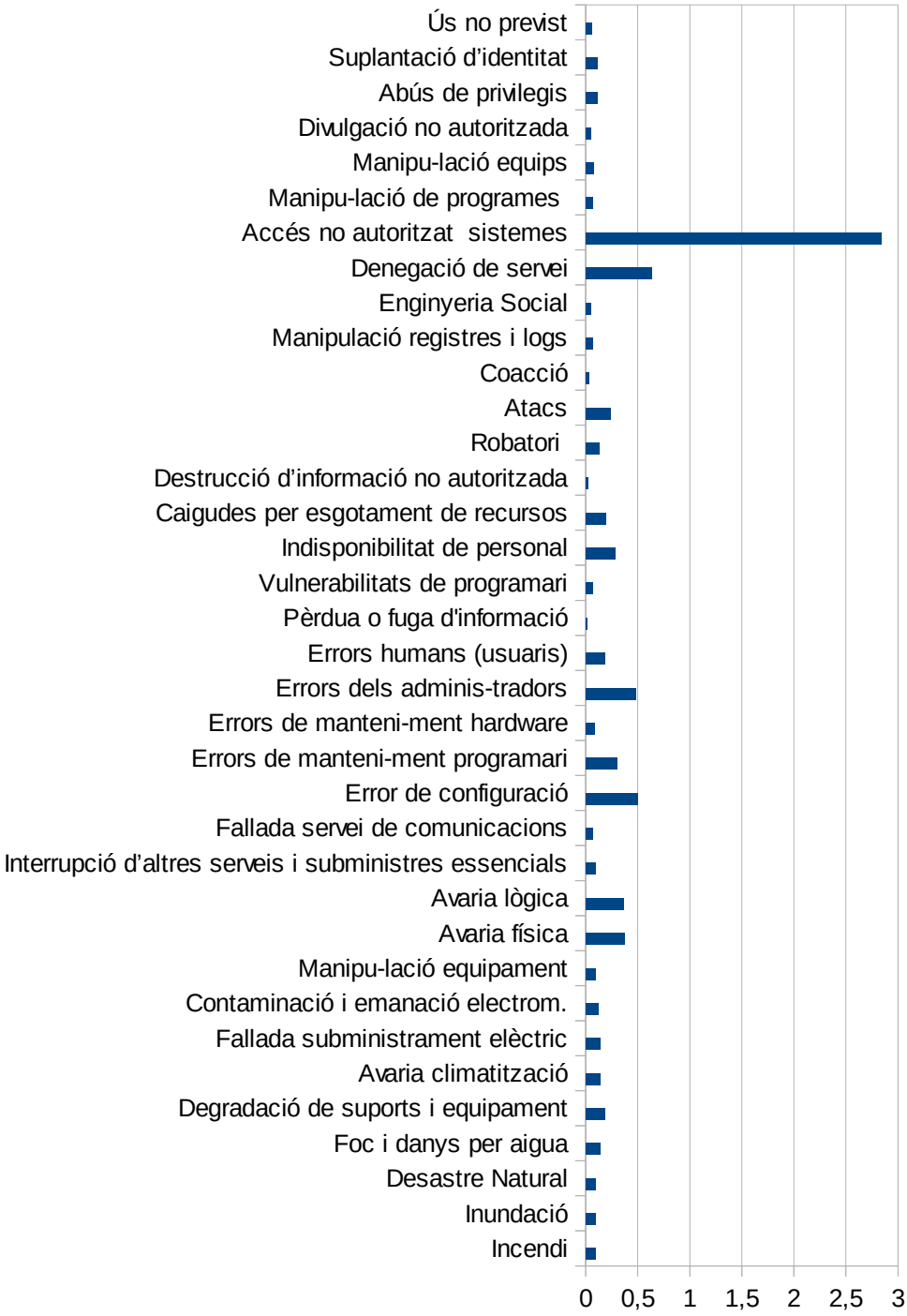


Es comprova d'entrada que l'amenaça més present correspon a la categoria d'atacs intencionats. Si analitzem amb més detall aquesta àrea obtenim:



Podem observar doncs que l'accés no autoritzat a sistemes constitueix una de les amenaces més rellevants destacant sobre les altres.

Taula d'amenaces segons el risc intrínsec:



Altres amenaces a tenir presents: Els atacs de denegació de servei, els errors de diferents persones i les avaries tant lògiques com físiques.

A continuació es mostraran els resultats dels actius els quals no es troben dins del risc acceptable:

Actius afectats			
Actiu	**Valor Qualitatiu**	**Llindar**	**Valor Risc**
Cabines de Disc	Molt Alt	50000	51600
Tallafocs	Alt	20000	25800
Desenvolupadors	Alt	20000	114000
Personal de sistemes i comunicacions	Alt	20000	71250
Switch	Mitjà	15000	21500
Worstations	Mitjà	15000	20640

Si ajustem els valors llindars per proximitat obtenim els següents actius susceptibles també a millora:

Freqüència			
Actiu	**Valor Qualitatiu**	**Llindar**	**Valor Risc**
Backup	Alt	20000	18525
Documentum	Alt	20000	18525
Antivirus	Mitjà	15000	13050
Ofimàtica	Mitjà	15000	13050

7.9 Resum executiu

L'anàlisi d'amenaces ha revelat una freqüència molt elevada de l'accés no autoritzat, la qual s'ha destacat. També en un segon nivell trobem els atacs de denegació de servei , errors i finalment averies. Aquest fet s'ha constat en el risc intrínsec, on observem que s'obtenen valoracions molt altes en el conjunt d'aplicacions, seguits de les dades i serveis.

Les mancances identificades que versen sobre els actius afectats són:

- Protecció indeguda de les aplicacions i serveis
- Disponibilitat deficient en la majoria d'actius
- Control deficient d'errors
- En general tots els sistemes són vulnerables als atacs i no estan protegits degudament
- Falta d'eines per l'anàlisi post-incident

Es proposen les següents accions correctores:

- Millorar la seguretat d'accessos a la informació així com la seva auditoria.
- Implementar noves polítiques i serveis per la protecció dels serveis i aplicacions.
- Crear procediments de programació de codi segur i entorns de desenvolupament segurs.
- Formar i capacitat el personal en la implementació de polítiques de seguretat.
- Crear procediments per minimitzar els errors.
- Control i gestió de xarxa activa.

Paral·lelament es realitzen les següents recomanacions:

- Garantir una política d'obligatorietat de distribució d'antivirus i una gestió centralitzada per administrar el seu desplegament.
- Revisar les polítiques de còpia de seguretat.
- Revisar i auditar el software utilitzat a l'organització.
- Garantir l'accés i la disponibilitat dels serveis .

8. Propostes de Projectes

8.1 Introducció

Per reduir el nivell de risc i establir un esquema de millora continua d'acord amb els requeriments de la norma ISO 27000:2013 es plantegen els següents projectes que es consideren prioritaris.

S'ha de considerar que els projectes fora de l'àmbit pròpiament de gestió TIC han quedat fora de l'abast d'aquest projecte.

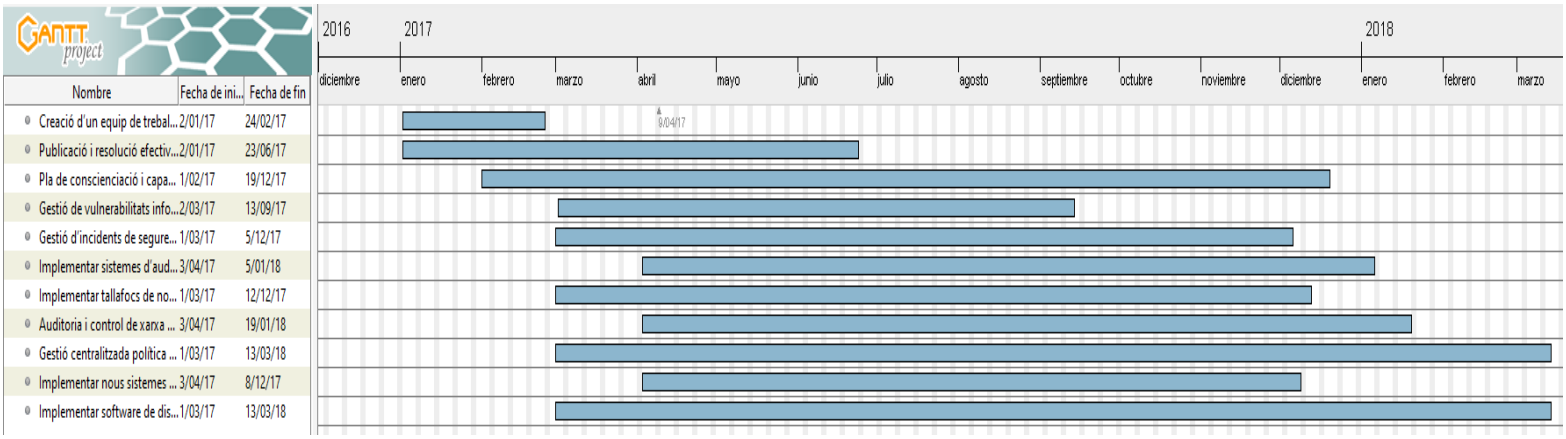
Es classificaran els projectes en dos grups principals. El primer estarà compost per aquells projectes que es troben fora del nivell de risc acceptable per l'organització. El segon grup estarà conformat per aquells projectes que tenen per objectiu millorar els nivells de seguretat de l'organització i permetre el compliment de la norma ISO 27001:2013 juntament amb altres normatives aplicables com les proposades per l'Ens nacional de seguretat[3].

PROJECTES DEL PLA DE TRACTAMENT DE RISCOS	PROJECTES COMPLEMENTARIS
Pla de conscienciació i capacitació del personal.	Creació d'un equip de treball en seguretat de la informació.
Gestió d'incidents de seguretat de la informació.	Publicació i resolució efectiva de les polítiques de seguretat.
Implementar sistemes d'auditories i anàlisi continuu sobre cabines de disc.	Gestió de vulnerabilitats informàtiques.
Implementar tallafocs de nova generació (capa 7) per poder implementar noves polítiques.	Gestió centralitzada política d'antivirus.
Auditoria i control de xarxa centralitzada.	Implementar nous sistemes de backup.
	Implementar software de distribució i inventari de software.

Els projectes es podran dur a terme de forma paral·lela donada la intervenció de diferents departaments. No obstant, es repartiran de forma progressiva en una visió anual.

El següent diagrama de Gantt representa el detall de la planificació dels projectes:

3 https://administracionelectronica.gob.es/ctt/ens#.WCoOW_l96Uk



Prioritització:

Definirem tres nivells de prioritització d'execució dels projectes:

- ALTA:
  - Creació d'un equip de treball en seguretat de la informació
  - Publicació i resolució efectiva de les polítiques de seguretat
- MITJA:
  - Pla de conscienciació i capacitació del personal
  - Gestió d'incidents de seguretat de la informació
  - Gestió de vulnerabilitats informàtiques
  - Implementar tallafocs de nova generació (capa 7) per poder implementar noves polítiques
  - Gestió centralitzada política d'antivirus
  - Implementar nous sistemes de backup
- BAIXA:
  - Implementar sistemes d'auditories i anàlisi continuu sobre cabines de disc
  - Auditoria i control de xarxa centralitzada
  - Implementar software de distribució i inventari de software

8.2 Descripció de les propostes

8.2.1 Creació d'un equip de treball en seguretat de la informació

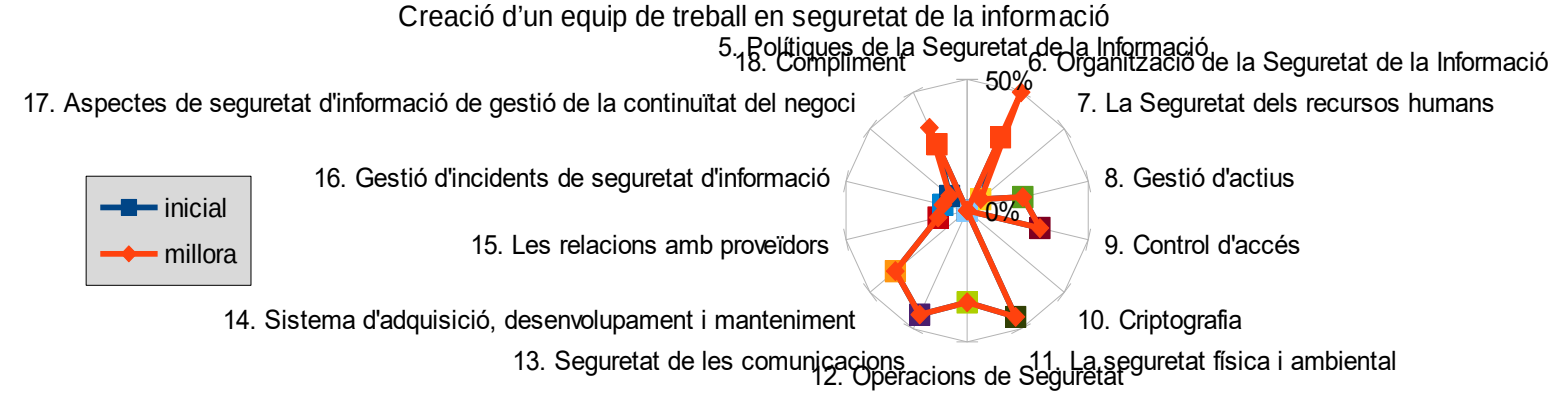
Objectiu: Crear un equip interdepartamental dins de l'àrea de tecnologia sobre el qual romandrà la responsabilitat i autoritat per la gestió i govern de la seguretat de la informació. Aquest objectiu bé limitat per la impossibilitat d'incorporar personal dedicat i la necessitat de participació de diferents àrees transversals.

Finalitat: Aconseguir un equip transversal i indisciplinar que incorpori tot els àmbits amb capacitat d'actuació respecte a la seguretat de la informació.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Definició de Requeriments	5 dies	500€
Aprovació de la creació de l'equip de treball	10 dies	1000€
Definició de responsabilitats	5 dies	500€
Assignació de personal	10 dies	1000€
Formació efectiva de l'equip de treball	10 dies	1000€
Total Projecte	40 dies	4000€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:

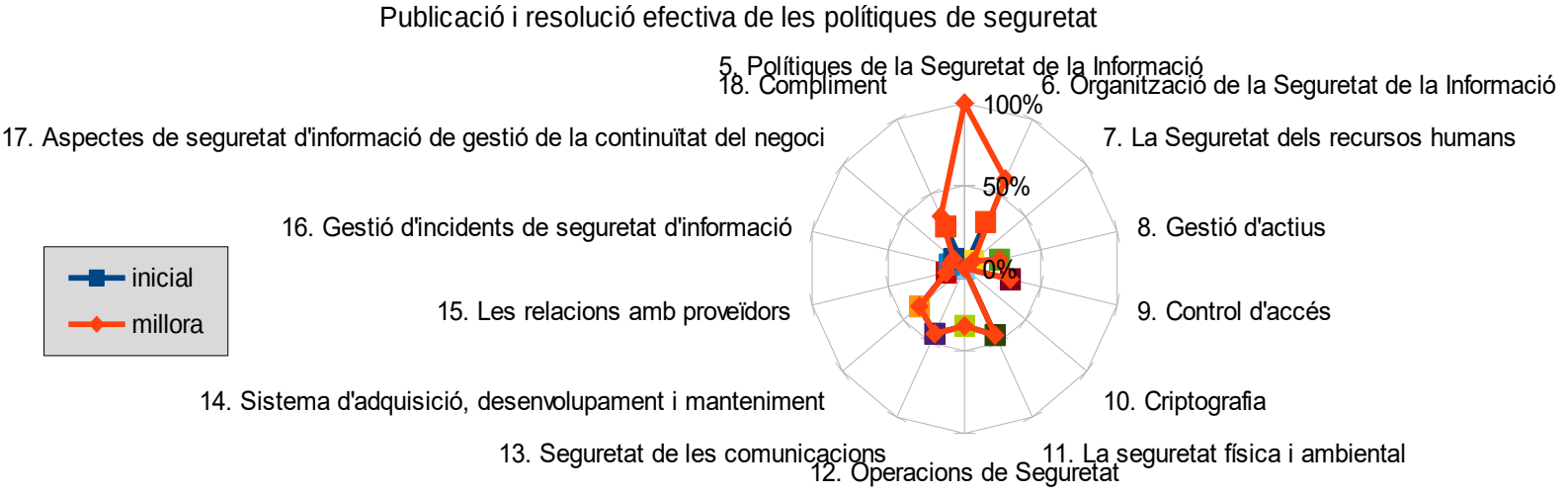


Finalitat: Aconseguir un acord en temes de seguretat acceptat per la direcció i amb el seu suport. Assentar les bases de la gestió de seguretat presents i futures.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Definició de la política general	30 dies	3000€
Revisió de la política per la direcció i comitès	15 dies	1500€
Aprovació de la política	10 dies	1000€
Publicació de les polítiques	20 dies	2000€
Divulgació de les polítiques	50 dies	5000€
Total Projecte	125 dies	12500€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



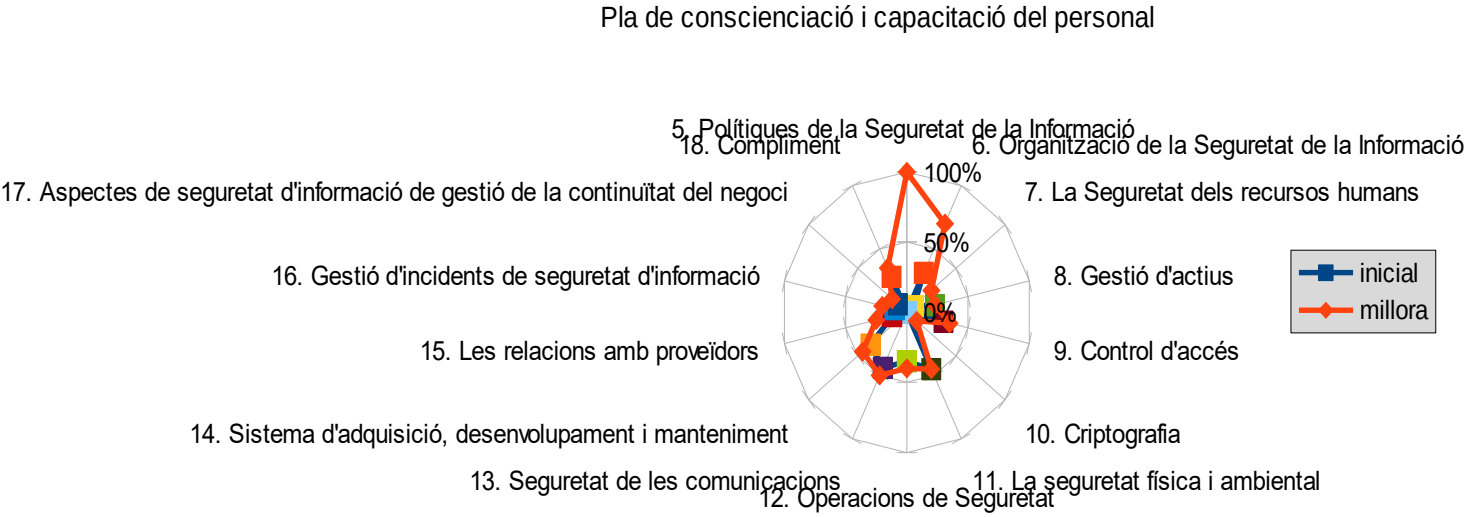
seguretat i de la millora continuada.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**

Definició del contingut i el públic objectiu	30 dies	3000€
Creació del material associat	30 dies	3000€
Formació al personal TIC	10 dies	1000€
Formació als administratius i funcionaris	30 dies	3000€
Formació als equips directius	10 dies	1000€
Proporcionar informació a proveïdors i tercers	30 dies	3000€
Programa de capacitació interna	60 dies	6000€
Recull de feedback dels plans de formació	15 dies	1500€
Anàlisi sobre els plans de formació i informació i el seu impacte	15 dies	1500€
Total Projecte	230 dies	23000€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



8.2.4 Gestió de vulnerabilitats informàtiques

Objectiu: Implementar processos de millora continua de vulnerabilitats informàtiques. Es preveu l'adquisició i posada en funcionament d'eines de suport a la gestió de vulnerabilitats.

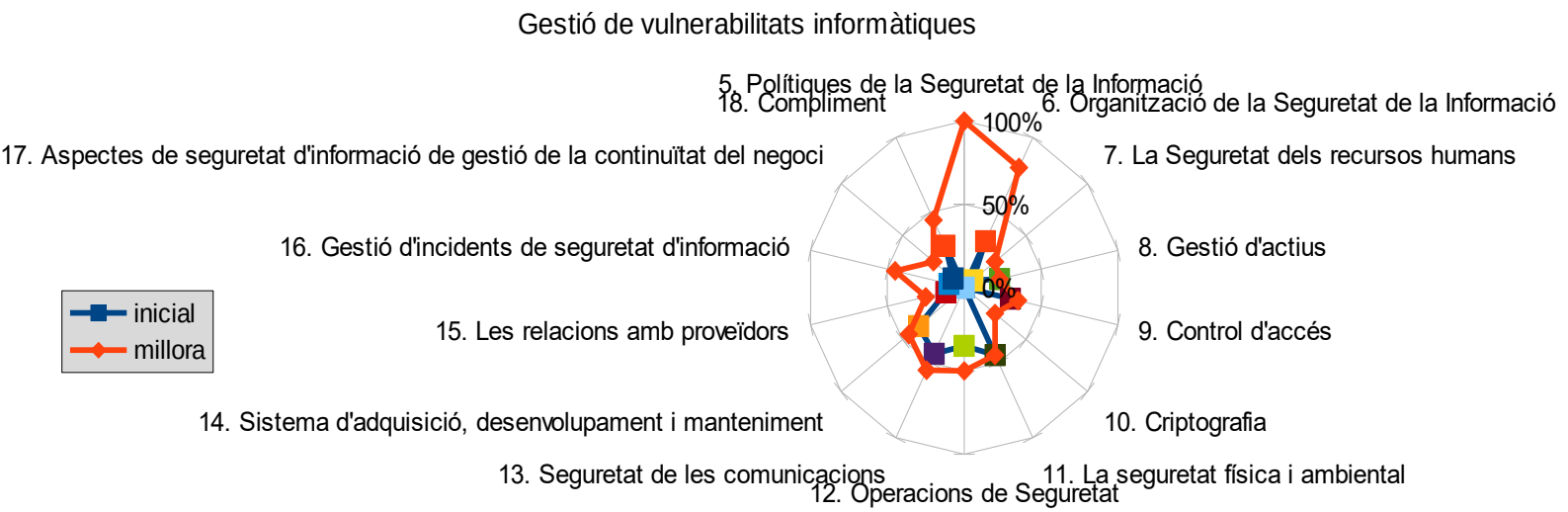
Finalitat: Adaptar dins els plans de millora continua la gestió de vulnerabilitats i adquirir capacitats necessàries per dur-les a terme.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Anàlisi de mercat i selecció de les eines	30 dies	3000€
Adquisició de les eines	10 dies	10000€
Instal·lació de l'aplicació	10 dies	500€
Formació del personal	30 dies	1000€
Configuració inicial i prova pilot	30 dies	1000€
Pla d'actuació i informes mensuals	30 dies	1000€

Total Projecte	140 dies	16500€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



8.2.5 Gestió d'incidents de seguretat d'informació

Objectiu: Alinear el servei de monitorització amb la correlació d'events de seguretat amb el suport extern d'empreses especialitzades.

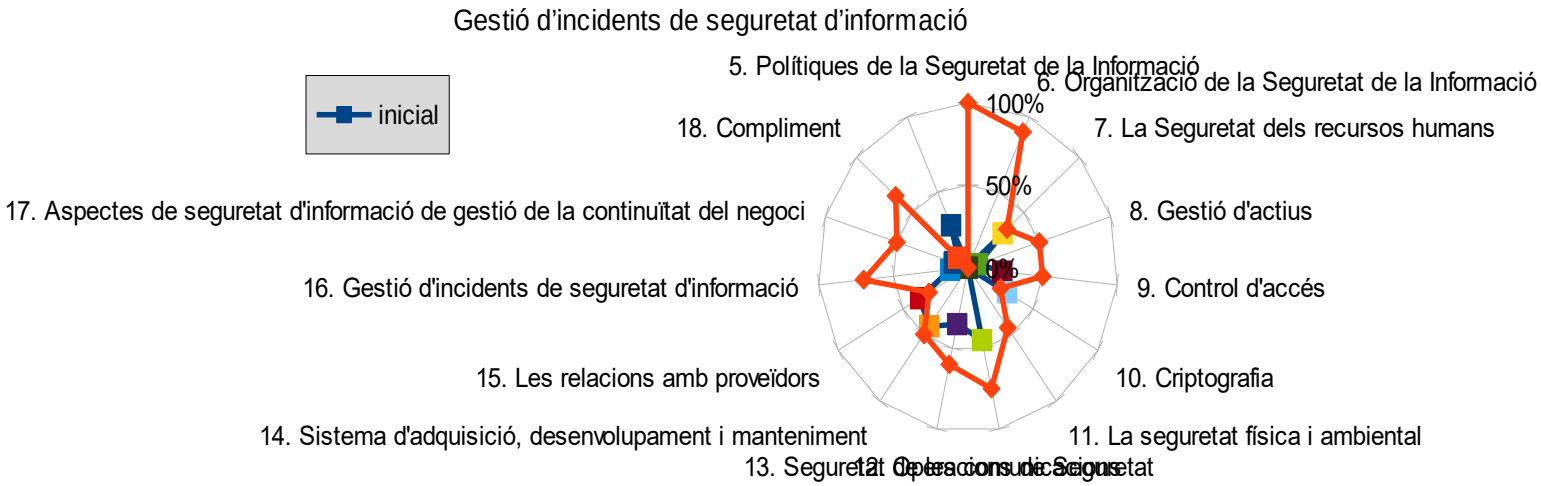
Finalitat: Adquirir la capacitat per poder anticipar els incidents de seguretat i actuar amb la màxima celeritat quan es produeixin.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Anàlisi de mercat i selecció de les eines i suport necessari	30 dies	3000€
Fase de concurs	90 dies	20000€
Resolució de concurs i selecció de	20 dies	500€

proveïdor		
Adaptació i configuració eines	30 dies	10000€
Prova pilot	30 dies	500€
Total Projecte	200 dies	34000€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



8.2.6 Implementar sistemes d'auditories i anàlisi continuu sobre cabines de disc

Objectiu: Implementació d'un producte que permeti la monitorització i auditoria en temps real del contingut de les cabines de disc tant si aquestes ofereixen sistemes de fitxers virtuals com físics. Aquest producte haurà de suportar diferents fabricants de cabines així com diferents sistemes de fitxers. Dins del projecte s'inclourà consultoria d'implementació externa.

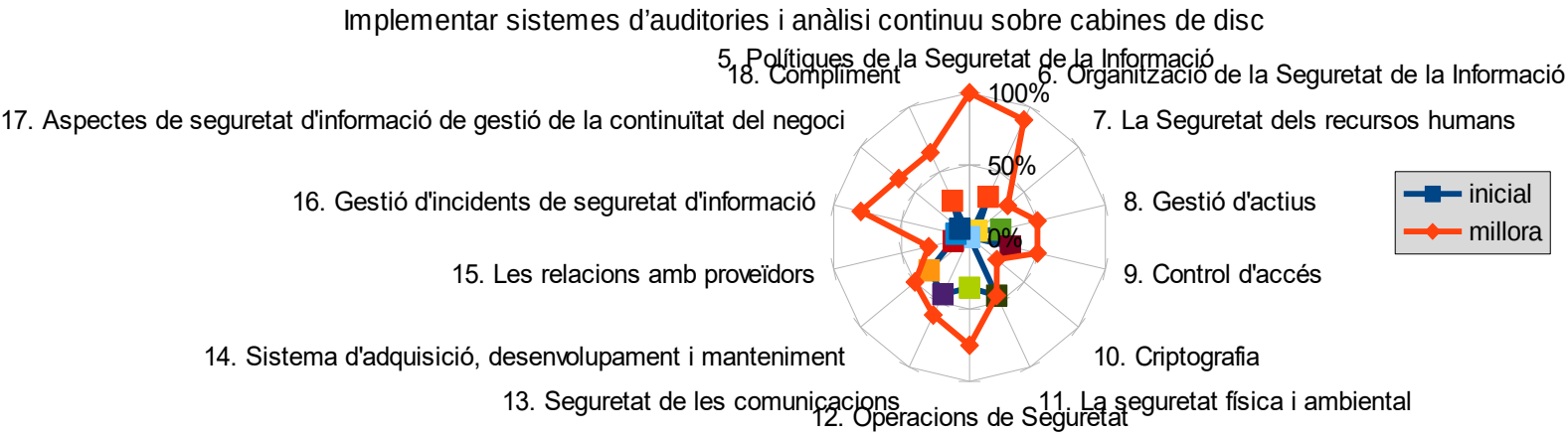
Finalitat: Acomplir els requisits legals amb aquelles dades susceptibles d'aplicació de la LOPD i capacitat d'anàlisi forense.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Anàlisi de mercat i selecció de les eines i suport necessari	30 dies	3000€

Fase de concurs	90 dies	20000€
Resolució de concurs i selecció de proveïdor	20 dies	500€
Adaptació i configuració eines	30 dies	10000€
Posada en producció escalonadament	30 dies	500€
Total Projecte	200 dies	34000€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



8.2.7 Implementar tallafocs de nova generació

Objectiu: Adquirir i implementar nous tallafocs perimetrals i interns de nova generació (capa 7). Permetran redefinir i ajustar les necessitats de connectivitat amb els avantatges de les eines incorporades de IPS i antivirus que permeten escanejar el trànsit en temps real juntament amb les eines d'auditoria de xarxa.

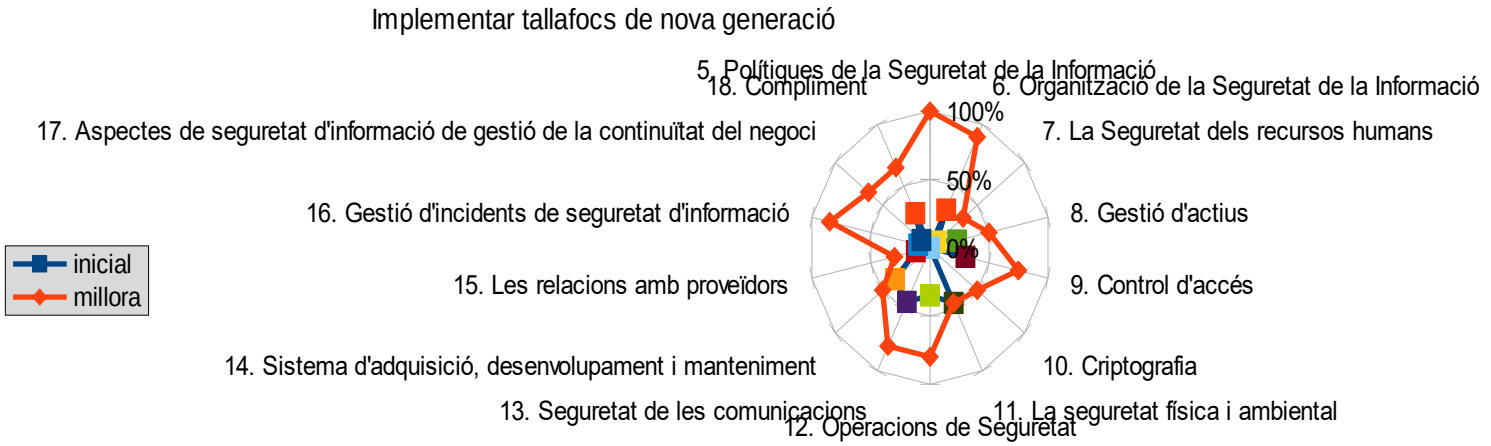
Finalitat: Adquirir les eines necessàries per proporcionar una correcte protecció als sistemes de la organització.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**

Anàlisi de mercat i selecció de les eines i suport necessari	30 dies	3000€
Fase de concurs	90 dies	100000€
Resolució de concurs i selecció de proveïdor	20 dies	500€
Adaptació i configuració eines	30 dies	10000€
Migració dels tallafocs	30 dies	500€
Nova parametrització (activació IPS)	5 dies	500€
Total Projecte	205 dies	114500€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:

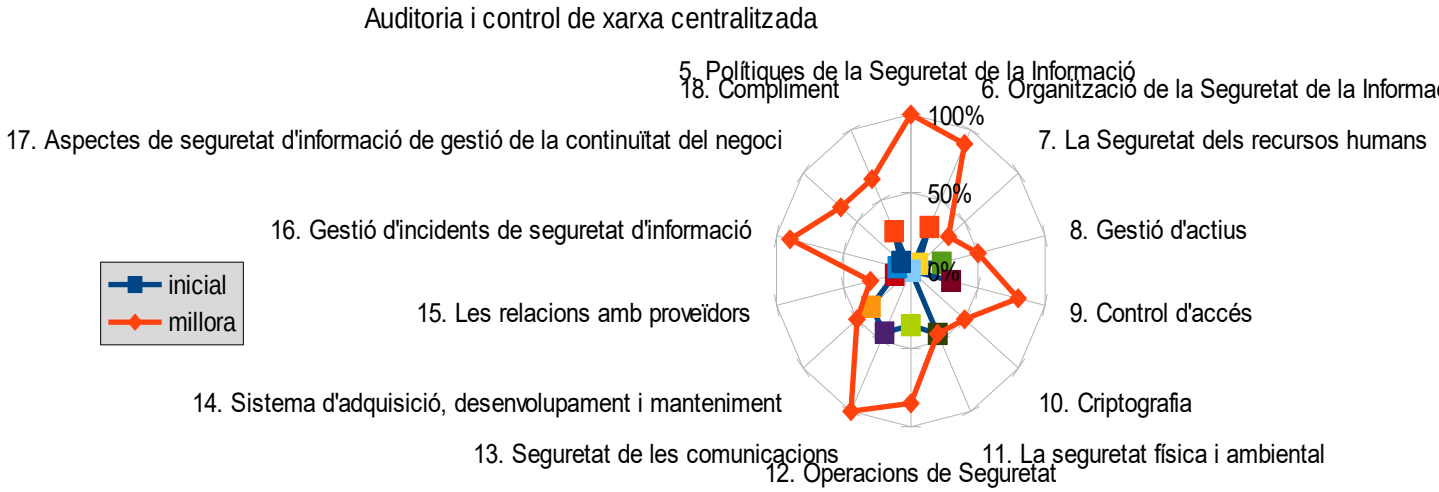


Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Anàlisi de mercat i selecció de les eines i suport necessari	30 dies	3000€
Fase de concurs	90 dies	50000€
Resolució de concurs i selecció de proveïdor	20 dies	500€

Adaptació i configuració eines	30 dies	10000€
Posada en funcionament	10 dies	500€
Incorporació progressiva de la infraestructura existent	30 dies	500€
Total Projecte	210 dies	114500€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:

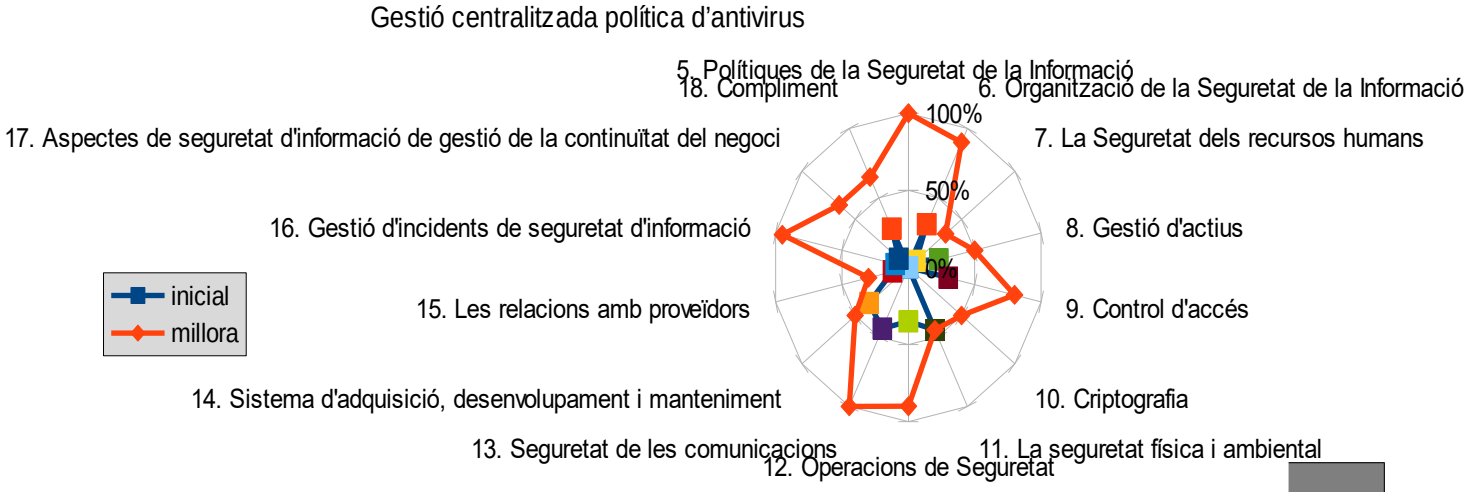


Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Anàlisi de mercat i selecció de les eines i suport necessari	30 dies	3000€
Fase de concurs	90 dies	30000€
Resolució de concurs i selecció de proveïdor	20 dies	500€
Adaptació i configuració eines	30 dies	10000€
Instal·lació del sevei	10 dies	500€
Incorporació progressiva dels clients existents	90 dies	1500€

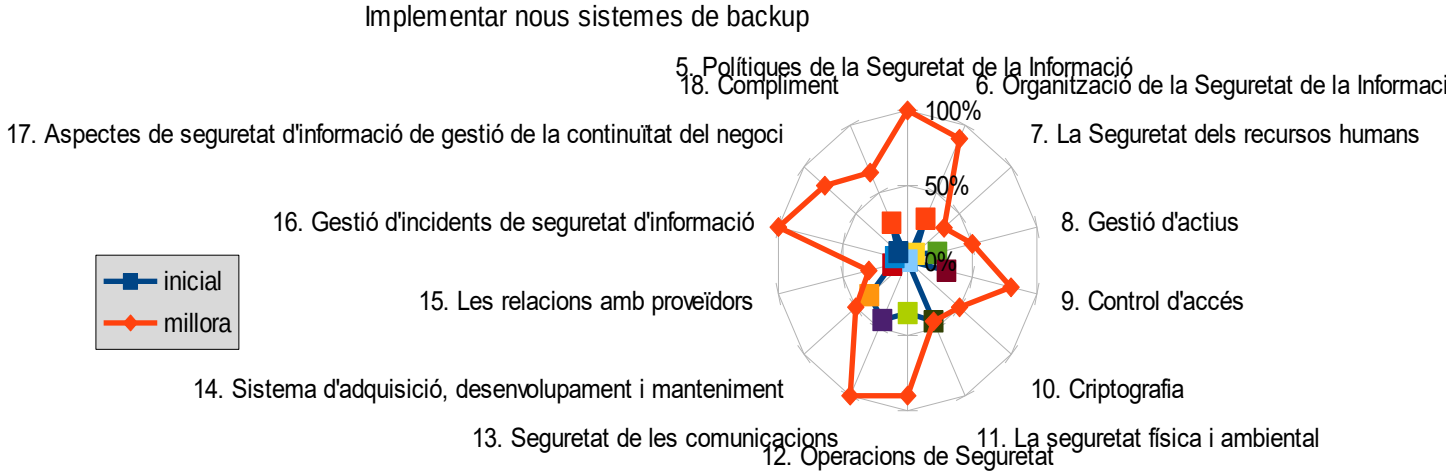
Total Projecte	270 dies	45500€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



Planificació		
Tasca	**Duració**	**Cost**
Anàlisi de mercat i selecció de les eines i suport necessari	30 dies	3000€
Fase de concurs	90 dies	50000€
Resolució de concurs i selecció de proveïdor	20 dies	500€
Adaptació i configuració eines	30 dies	10000€
Instal·lació	10 dies	500€
Incorporació progressiva dels filesystems existents	60 dies	1500€
Total Projecte	180 dies	65500€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



8.2.11 Implementar software de distribució i inventari de software

Objectiu: Avaluar i adquirir una solució que permeti centralitzar la gestió activa del software instal·lat en els equips. Aquesta solució hauria de permetre conèixer amb fiabilitat tot aquell software instal·lat en els equips de l'organització així com proporcionar informes detallats. L'inventari d'aplicacions (i hardware) permetrà obtenir una visió detallada de l'ús dels equips i adquirir control sobre les aplicacions que instal·len els propis usuaris.

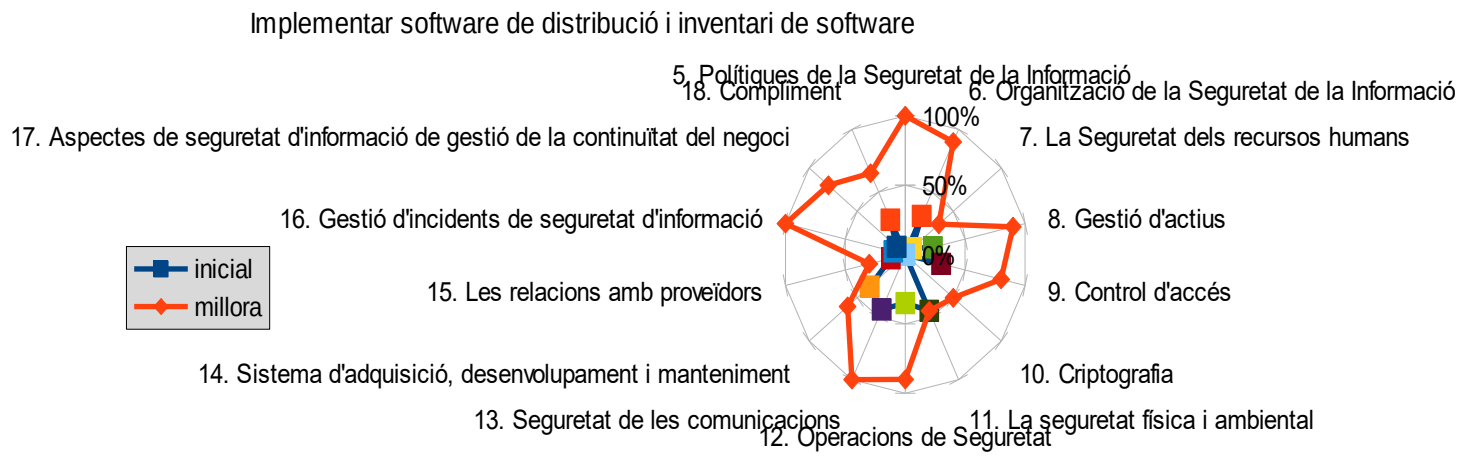
Finalitat: Obtenir el coneixement del software usat a la organització i garantir-ne una distribució controlada i segura.

Planificació proposada:

Planificació		
Tasca	**Duració**	**Cost**
Anàlisi de mercat i selecció de les eines i suport necessari	30 dies	3000€

Fase de concurs	90 dies	30000€
Resolució de concurs i selecció de proveïdor	20 dies	500€
Adaptació i configuració eines	30 dies	10000€
Instal·lació del servei	10 dies	500€
Incorporació progressiva dels clients existents	90 dies	1500€
Total Projecte	270 dies	45500€

A la finalització d'aquest projecte els nivells de maduresa dels dominis de seguretat es veurà modificat de la següent forma:



9. Auditoria de compliment

9.1. Introducció

El propòsit d'aquesta auditoria és identificar el nivell de compliment del SGSI de la UNIF respecte als controls i clàusules de la norma internacional ISO 27002. Aquesta auditoria es realitza un cop ha finalitzat la implementació dels projectes proposats i té un caràcter d'auditoria inicial.

La ISO 27002 analitza la seguretat de la informació d'una organització, sigui del tipus que sigui i independentment de les seves dimensions. La ISO s'agrupa amb 114 controls o mesures preventives , organitzades en 14 àrees i 35 objectius.

El resultat de l'auditoria estableix l'estat de seguretat d'una organització en un moment donat del temps en tots els àmbits de protecció: físic, lògic, organitzatiu i legal. Concretament els resultats d'aquesta auditoria proporcionen una sèrie de "No Conformitats", "No Conformitats Menors" i "Millores/Recomanacions" que seran utilitzades per a la fase de millora continua del SGSI. Posteriorment , al cap d'un temps es tornaran a revisar seguint els cicles de millora continua.

A l'ANNEX XI es pot trobar l'informe d'auditoria.

9.2. Metodologia

La normativa utilitzada per du a terme l'auditoria es basa en els 114 controls o mesures preventives organitzades en 14 àrees i 35 objectius de control de la i ISO/IEC 27002. Aquests controls ens permetran conèixer l'estat actual de la Organització en relació a la Seguretat de la Informació.

La valoració es realitzarà segons el model de maduresa de la capacitat (CMM). La següent taula mostra els barems utilitzats:

MADURESA (CMM)	EFECTIVITAT	DESCRIPCIÓ
Inexistent	0 %	Carència completa de qualsevol procés que reconeguem.
Inicial	10%	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal.
Reproduïble, però intuïtiu	50%	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca.
Procés definit	90%	La organització sencera participa al procés.
Gestionat y mesurable	95%	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.

Optimitzat	100%	Els processos estan sota constant millora.

Aquesta auditoria s'ha realitzat seguint les indicacions del Pla d'Auditoria establert. Les tasques han consistit en:

- Recollida d'Informació: Petició de tota la documentació rellevant per l'auditoria. Revisió la seva idoneïtat i vigència, a més que es trobi alineada amb les bones pràctiques especificades per la ISO.
- Execució de proves d'auditoria.
    - Realització de qüestionaris (entrevistes) amb els responsables de servei.
    - Visites de les instal·lacions, incloent els centres de càlcul.
    - Verificació de controls.
- Anàlisi de la informació i elaboració d'Informe final: Anàlisi de la informació recollida en les diferents proves i entrevistes. Aquest anàlisi determinarà el nivell de maduresa i compliment respecte a la ISO 27002.
- Redacció d'informe: Informe final on es descriuen les diferents No Conformitats i recomanacions de millora.

9.3. Avaluació de la maduresa

L'objectiu d'aquesta fase és avaluar la maduresa de la seguretat respecte als diferents dominis de control descrits per la ISO/IEC 27002:2013.

Per mesurar el grau de maduresa s'ha utilitzat el model CMM seguint el model de la fase d'anàlisis diferencial. S'establiran uns percentatges que permetran identificar el progrés realitzat en cada un dels controls auditats.

ÀREA	CMM (Anterior)	CMM (Futura)
5. Polítiques de la Seguretat de la Informació	0%	90%
6.Organització de la seguretat de la informació	31%	50%
7. La seguretat dels recursos humans	7%	50%
8. Gestió d'actius	23%	95%

9. Control d'accés	30%	50%
10.Criptografia	0%	50%
11.La seguretat física i ambiental	45%	50%
12.Operacions de Seguretat	35%	90%
13.Seguretat de les comunicacions	44%	95%
14.Sistema d'adquisició, desenvolupament i manteniment	37%	50%
15.Les relacions amb proveïdors	12%	50%
16.Gestió d'incidents de seguretat d'informació	10%	95%
17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	9%	90%
18.Compliment	28%	95%

9.4. Resultats

Taula de resultats obtinguts:

CONTROLS	CONFORMITATS
5.1 Direcció de gestió de seguretat de la informació	CONFORME
6.1 Organització interna	CONFORME
6.2 Els dispositius mòbils i el teletreball	NO CONFORME
7.1 Amb anterioritat a l'ocupació	NO CONFORME
7.2 Durant l'ocupació	CONFORME
7.3 Terminació i canvi d'ocupació	NO CONFORME
8.1 La responsabilitat dels actius	CONFORME
8.2 Classificació de la Informació	CONFORME

8.3 Mitjans de manipulació	CONFORME
9.1 Els requisits de negoci de control d'accés	NO CONFORME
9.2 Gestió d'accés dels usuaris	CONFORME
9.3 Responsabilitat dels usuaris	CONFORME
9.4 Sistema de control i d'accés a les aplicacions	CONFORME
10.1 Controls criptogràfics	CONFORME
11.1 Les àrees segures	CONFORME
11.2 Equip	NO CONFORME
12.1 Procediments i responsabilitats operacionals	CONFORME
12.2 Protecció contra el malware	CONFORME
12.3 Còpia de seguretat	CONFORME
12.4 Registre i supervisió	CONFORME
12.5 de control de programari operacional	CONFORME
12.6 La gestió tècnica de la vulnerabilitat	CONFORME
12.7 Sistemes d'informació consideracions d'auditoria	NO CONFORME
13.1 De gestió de seguretat de xarxa	CONFORME
13.2 La transferència d'informació	CONFORME
14.1 Els requisits de seguretat dels sistemes d'informació	CONFORME
14.2 Seguretat en els processos de desenvolupament i suport	CONFORME
14.3 Les dades de prova	NO CONFORME
15.1 Seguretat de la informació en relació amb els proveïdors	NO CONFORME
15.2 La gestió de la prestació de serveis de proveïdors	CONFORME
16.1 Gestió dels incidents de seguretat de la informació i millores	CONFORME

17.1 La continuïtat seguretat de la informació	CONFORME
17.2 Les redundàncies	CONFORME
18.1 El compliment dels requisits legals i contractuals	CONFORME
18.2 Opinions seguretat de la informació	CONFORME

Els resultats de l'anàlisi de cada un dels controls de la ISO27002 mostren un total de **8** "No Conformitats" que hauran de ser corregides:

- 6.2 Els dispositius mòbils i el teletreball
- 7.1 Amb anterioritat a l'ocupació
- 7.3 Terminació i canvi d'ocupació
- 9.1 Els requisits de negoci de control d'accés
- 11.2 Equip
- 12.7 Sistemes d'informació consideracions d'auditoria
- 14.3 Dades de prova
- 15.1 Seguretat de la informació en relació amb els proveïdors

Detall:

NUMERAL DE LA NORMA	DESCRIPCIÓ NORMA	DESCRIPCIÓ	TIPOLOGIA
6.2.1	Polítiques per dispositius mòbils	No està definida cap política ni normativa al respecte. No es realitza cap tipus de control.	NO CONFORME
6.2.2	Teletreball	No està definida cap política ni normativa al respecte. No es realitza cap tipus de control.	NO CONFORME
6.2.2	Teletreball	Revisió i millora del servei VPN	MILLORA
7.1.2	Termes i condicions d'ocupació	Existència de procediments de contractació sense acords de confidencialitat en alguns departaments.	NO CONFORMITAT MENOR
7.3.1	Finalització o canvi de les responsabilitats d'ocupació	No es revisa els materials en possessió de l'empleat quan	NO CONFORME

		aquest finalitza la prestació de serveis.	
9.1.1	Política de control d'accés	No es realitzen controls d'accés físic suficient.	NO CONFORMITAT MENOR
11.2.5	Retirada dels actius	No existeix procediment	NO CONFORMITAT
11.2.6	Seguretat dels equips i actius fora de les instal·lacions	No existeix procediment ni mesures de seguretat addicionals.	NO CONFORMITAT
11.2.7	L'eliminació segura o la reutilització dels equips	No existeix procediment establert.	NO CONFORMITAT MENOR
11.2.9	Netejar l'escriptori i la política de pantalla transparent	No s'aplica actualment de forma homogènia.	MILLORA
12.7.1	Sistemes d'informació controls d'auditoria	No es disposen de les eines adequades per realitzar auditories.	NO CONFORMITAT MENOR
14.3.1	Protecció de dades de prova	S'identifiquen dades reals en entorns de preproducció.	NO CONFORMITAT MENOR
15.1.1	Política de seguretat de la informació de relacions amb els proveïdors	No s'inclouen clausules específiques de seguretat en els acords de prestació de serveis.	NO CONFORMITAT
15.1.2	Abordar la seguretat dins dels acords amb proveïdors	No s'inclouen clausules específiques de seguretat en els acords de prestació de serveis.	NO CONFORMITAT MENOR
15.2.1	Seguiment i revisió dels serveis de proveïdors	No es realitza seguiment.	MILLORA

L'auditoria realitzada en el Sistema de Gestió de Seguretat de la Informació de la UNIF es van trobar:

- 4 No Conformitats
- 6 No Conformitats Menors
- 2 3 Millores

Cal indicar que la majoria de controls de la norma es troben dins del llindar establert per la UNIF en el seu pla de tractament de riscos. Les No Conformitats que s'han detallat s'hauran de revisar en futures auditories.

10. Conclusions

Durant el desenvolupament d'aquest projecte s'han establert les bases que permetran la implementació d'un Sistema de Gestió de la Seguretat de la Informació.

Inicialment es va realitzar una reducció de l'abast i conseqüentment dels actius analitzats. Es va incloure en el projecte només aquells elements provinents dels serveis centrals de la universitat i es va excloure tota la resta. Aquesta decisió es va prendre en base a l'escàs marge de temps per realitzar el projecte i al desconeixement general de l'abast que podria suposar, atès que actualment equipaments com per exemple el destinat a la recerca superen en escreix els dels serveis centrals.

La planificació prevista ha sigut suficient per complir amb les dates les fases d'entrega. No obstant, l'adequació d'aquestes han condicionat el desenvolupament del projecte.

Els aspectes a millorar versen inicialment sobre el detall dels actius, especialment aquells referents a la informació o dades. El desconeixement de moltes àrees, i els seus actius relacionats, impedeixen realitzar una valoració adient i com a resultat les mesures seleccionades segurament serien diferents, o com a mínim s'establirien prioritats diferents.

Els progressos aconseguits per la implantació del SGSI són:

- Determinar l'actual estat de la seguretat de la informació en relació als diferents aspectes de la ISO 27002.
- Determinar les responsabilitats de cada membre de l'estructura organitzativa designada per gestionar la seguretat.
- Identificar els actius crítics de l'organització, determinar les amenaces a què estan exposats i, avaluar els riscos als que estan exposats els diferents elements del SGSI.
- Seleccionar, prioritzar i proposar un conjunt de projectes i mesures que permetran millorar la seguretat de l'organització.

L'organització ha de seguir treballant atès que aquest SGSI forma part d'un procés de millora contínua en constant actualització i evolució. El futur està marcat per l'aprofundiment de l'anàlisi de riscos amb la resta d'actius juntament amb altres tipus d'amenaces als que estem exposats.

11. Glossari

Definició dels termes més rellevants:

Amenaça: Qualsevol circumstància o esdeveniment amb el potencial de tenir un impacte negatiu operacions de l'organització, actius de l'organització, els individus, altres organitzacions o la nació a través d'un sistema d'informació a través d'un accés no autoritzat, destrucció, divulgació, modificació de la informació, i / o denegació de servei.

Anàlisis de Riscos: Procés d'identificació dels riscos per a la seguretat del sistema i la determinació de la probabilitat d'ocurrència, l'impacte resultant, i les mesures de seguretat addicionals que mitiguin aquest impacte.

Auditoria: Procés independent, documentat i sistemàtic per obtenir evidència d'auditoria i avaluar-la objectivament per determinar el grau en el qual un criteri d'auditoria és complert.

Atac: Intent de destruir, exposar, deshabilitar, alterar, o aconseguir accés no autoritzat o de fer un ús no autoritzat d'un actiu.

Control d'Accés: Mitjà per assegurar que l'accés a l'actiu és autoritzat i restringit d'acord als requeriments del negoci i de la seguretat.

Confidencialitat: Propietat de la informació que no sigui revelada i es faci disponible a individus, entitats o processos no autoritzats.

Competència: Habilitat per aplicar coneixement i aptituds per aconseguir un resultats establerts.

Control: Mesura que modifica el risc.

Disponibilitat: Propietat de la informació de ser accessible i utilitzable sota demanda per una entitat autoritzada.

Informació: Conjunt de dades que tenen sentit, i que són considerats un actiu més dins de les organitzacions.

Informació documentada: Informació que requereix ser controlada i mantinguda per una organització i el mitjà en el qual està continguda.

Integritat: Propietat d'exactitud i completesa.

Millora Contínua: Activitat recurrent per millorar l'acompliment.

Norma ISO 27002:2013: Versió de l'any 2013 de la norma ISO 27002 dissenyada perquè les organitzacions la usin com un marc de referència per seleccionar controls dins del procés d'implementació d'un Sistema de Gestió de la Seguretat de la Informació.

Parts Interessades: Persones o organitzacions que són o poden ser afectades per una decisió o activitat.

Seguretat de la Informació: La Seguretat de la informació involucra l'aplicació i gestió de les mesures apropiades de seguretat que tinguin en compte un ampli rang d'amenaces. La seguretat de la informació és aconseguida per mitjà de la implementació d'un conjunt

aplicable de controls, seleccionats per mitjà d'un procés de gestió de riscos i gestionats usant un Sistema de Gestió de Seguretat de la Informació, incloent polítiques, processos, procediments, programari o maquinari per protegir els actius d'informació identificats.

Sistema de Gestió: Conjunt d'elements que interactuen i s'interrelacionen per establir polítiques i objectius i els processos per aconseguir aquests objectius.

Tolerància al risc: El nivell de risc que una entitat està disposat a assumir per tal d'aconseguir un resultat potencial desitjat.

Triagge: Activitat dins del procediment de resposta a incidents en la qual s'analitza l'esdeveniment per detectar si és o no un incident de seguretat, addicionalment si l'esdeveniment efectivament és un incident, aquest es classifica d'acord al seva gravetat amb la finalitat de prendre les decisions corresponents per al seu tractament.

Vulnerabilitat: Feblesa en un actiu o control que pot ser explotada per una o més amenaces.

12. Bibliografia

MISTIC assignatura Sistemes de Gestió de la Seguretat

MISTIC assignatura Auditoria

INTECO Instituto Nacional de Tecnologías de la Información

http://www.inteco.es

CONTROLS ISO 27002

http://iso27000.es/iso27002.html

MAGERIT

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WEL3RPl96Uk

ESQUEMA NACIONAL DE SEGURIDAD

https://administracionelectronica.gob.es/ctt/ens#.WEQwn_l96Uk

ANNEX I Anàlisi diferencial

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
5	POLÍTIQUES DE SEGURETAT	0%		
5.1	Direcció de la gestió de seguretat de la informació	0%		Proporcionar orientació i suport per a seguretat de la informació, d'acord amb els requeriments del negoci i les lleis i reglaments pertinents de gestió.
5.1.1	Polítiques de seguretat de la informació	0%	Inexistent	
5.1.2	Revisió de les polítiques de seguretat de la informació	0%	Inexistent	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
6	ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ	31%		
6.1	Organització interna	57%		Establir un marc de gestió per iniciar i controlar la implementació i operació de seguretat de la informació dins de l'organització.
6.1.1	Rols i responsabilitats de seguretat de la informació	10%	Inicial	
6.1.2	Separació de funcions	90%	Definit	
6.1.3	Contacte amb les autoritats	90%	Definit	
6.1.4	Contacte amb els grups d'interès especial	95%	Gestionat	
6.1.5	Seguretat de la informació en la gestió de projectes	0%	Inexistent	

6.2	Dispositius mòbils i teletreball	5%		Garantir la seguretat del teletreball i l'ús de dispositius mòbils.
6.2.1	Polítiques per dispositius mòbils	0%	Inexistent	
6.2.2	Teletreball	10%	Inicial	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
7	SEGURETAT DELS RECURSOS HUMANS	7%		
7.1	Amb anterioritat a l'ocupació	10%		Garantir que els empleats i contractistes són adequats per a les funcions per a les que estan considerades.
7.1.1	Control de Selecció	10%	Inicial	
7.1.2	Termes i condicions d'ocupació	10%	Inicial	
7.2	Durant l'ocupació	10%		Garantir que els empleats i contractistes són conscients de les seves responsabilitats i compleixin amb la seguretat de la informació
7.2.1	Responsabilitats de gestió i direcció	10%	Inicial	
7.2.2	Conscienciació sobre la seguretat de la informació, l'educació i la formació	10%	Inicial	
7.2.3	Procés disciplinari	10%	Inicial	
7.3	Terminació i canvi d'ocupació	0%		Protecció dels interessos de l'organització com a part del procés de canviar o acabar la feina.
7.3.1	Finalització o canvi de les responsabilitats d'ocupació	0%	Inexistent	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
8	GESTIÓ D'ACTIUS	23%		
8.1	Responsabilitat dels actius	57%		Identificar els actius de l'organització i definir les responsabilitats de protecció adequades
8.1.1	Inventari d'actius	90%	Definit	
8.1.2	Propietat dels actius	90%	Definit	
8.1.3	Ús acceptable dels actius	0%	Inexistent	
8.1.4	Devolució d'actius	50%	Repetible	
8.2	Classificació de la Informació	10%		Garantir que la informació rebi un nivell adequat de protecció d'acord amb la seva importància per a l'organització.
8.2.1	Classificació de la informació	10%	Inicial	
8.2.2	Etiquetatge de la informació	10%	Inicial	
8.2.3	Manipulació dels actius	10%	Inicial	
8.3	Gestió dels mitjans físics.	0%		Evitar la divulgació no autoritzada, modificació, eliminació o destrucció de la informació emmagatzemada en els mitjans de comunicació.
8.3.1	Gestió de suports extraïbles	0%	Inexistent	
8.3.2	Eliminació dels mitjans	0%	Inexistent	
8.3.3	Transferència de mitjans físics	0%	Inexistent	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
9	CONTROL D'ACCÉS	30%		
9.1	Requisits de negoci de control d'accés	50%		limitar l'accés a les instal·lacions de processament d'informació i d'informació.

9.1.1	Política de control d'accés	50%	Repetible	
9.1.2	L'accés a les xarxes i serveis de xarxa	10%	Inicial	
9.2	Gestió d'accés dels usuaris	37%		Garantir l'accés d'usuaris autoritzats i evitar l'accés no autoritzat als sistemes i serveis
9.2.1	Registre d'usuaris i baixes	50%	Inicial	
9.2.2	Aprovisionament d'accés als usuaris	10%	Inicial	
9.2.3	Gestió de drets d'accés privilegiats	10%	Inicial	
9.2.4	Gestió de la informació de connexió de secret dels usuaris	90%	Definit	
9.2.5	Revisió dels drets d'accés dels usuaris	10%	Inicial	
9.2.6	Eliminació o ajust dels drets d'accés	50%	Repetible	
9.3	Responsabilitat dels usuaris	0%		Responsabilització dels usuaris per guardar la informació d'accés.
9.3.1	Ús del control de la informació de connexió secreta	0%	Inexistent	
9.4	Sistema de control i d'accés a les aplicacions	34%		Prevenir l'accés no autoritzat a sistemes i aplicacions.
9.4.1	Restricció d'accés a la informació	10%	Inicial	
9.4.2	Procediments de registre segur	50%	Repetible	
9.4.3	Sistema de gestió de contrasenyes	90%	Definit	
9.4.4	Ús dels programes, utilitats privilegiades	10%	Inicial	

9.4.5	Control d'accés al codi font del programa	10%	Inicial	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
10	CRIPTOGRAFIA	0%		
10.1	Controls criptogràfics	0%		Garantir l'ús adequat i eficaç de la criptografia per protegir la confidencialitat, autenticitat i la integritat de la informació.
10.1.1	Política sobre l'ús de controls criptogràfics	0%	Inexistent	
10.1.2	Gestió de claus	0%	Inexistent	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
11	SEGURETAT FÍSICA I DE L'ENTORN	45%		
11.1	Àrees segures	48%		Prevenir l'accés no autoritzat físicament, danys i interferències a les instal·lacions de processament d'informació i la informació de l'organització.
11.1.1	Perímetre de seguretat física	50%	Repetible	
11.1.2	Controls d'entrada físics	50%	Repetible	
11.1.3	Protecció d'oficines, sales i instal·lacions	50%	Repetible	
11.1.4	Protecció contra amenaces externes i ambientals	50%	Repetible	
11.1.5	Treball en àrees segures	0%	Inexistent	
11.1.6	Lliurament i càrrega de les zones	90%	Definit	
11.2	Equips	43%		Evitar la pèrdua, dany, robatori dels actius i la interrupció de les operacions de l'organització.

11.2.1	Ubicació i protecció dels equips	90%	Definit	
11.2.2	Serveis de subministrament	50%	Repetible	
11.2.3	La seguretat de cablejat	90%	Definit	
11.2.4	El manteniment de l'equip	50%	Repetible	
11.2.5	Retirada dels actius	90%	Definit	
11.2.6	Seguretat dels equips i actius fora de les instal·lacions	0%	Inexistent	
11.2.7	L'eliminació segura o la reutilització dels equips	10%	Inicial	
11.2.8	Equip d'usuari desatès	10%	Inicial	
11.2.9	Netejar l'escriptori i la política de pantalla transparent	0%	Inexistent	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
12	OPERACIONS DE SEGURETAT	35%		
12.1	Procediments i responsabilitats operacionals	50%		Garantir operacions correctes i segures d'instal·lacions de processament d'informació.
12.1.1	Procediments operacionals documentats	50%	Repetible	
12.1.2	Gestió de canvis	10%	Inicial	
12.1.3	Gestió de la capacitat	50%	Repetible	
12.1.4	Separació entorns de desenvolupament, prova i operacions	90%	Definit	

12.2	Protecció contra el codi maliciós	50%		Garantir que les instal·lacions de processament d'informació i la informació estan protegits contra el codi maliciós.
12.2.1	Controls contra el codi maliciós.	50%	Repetible	
12.3	Còpia de seguretat	95%		Evitar la pèrdua de dades.
12.3.1	Informació de còpia de seguretat	95%	Gestionat	
12.4	Registre i supervisió	50%		Registrar els esdeveniments i generar evidència.
12.4.1	Registre d'esdeveniments	50%	Repetible	
12.4.2	Protecció de la informació de registre	50%	Repetible	
12.4.3	Administrador i operador registres	10%	Inicial	
12.4.4	Sincronització del rellotge	90%	Definit	
12.5	Control de programari operacional	0%		Garantir la integritat dels sistemes operatius.
12.5.1	Instal·lació de programari en sistemes operatius	0%	Inexistent	
12.6	Gestió tècnica de vulnerabilitats	0%		Prevenir l'explotació de vulnerabilitats tècniques
12.6.1	Gestió de vulnerabilitats tècniques	0%	Inexistent	
12.6.2	Restriccions en la instal·lació del programari	0%	Inexistent	
12.7	Sistemes d'informació consideracions d'auditoria	0%		Minimitzar l'impacte de les activitats d'auditoria en els sistemes operatius.

12.7.1	Sistemes d'informació controls d'auditoria	0%	Inexistent	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
13	SEGURETAT DE LES COMUNICACIONS	44%		
13.1	Gestió de seguretat de xarxa	77%		Garantir la protecció de la informació a la xarxa i les instal·lacions de suport de processament d'informació.
13.1.1	Controls de xarxa	90%	Definit	
13.1.2	Seguretat dels serveis de xarxa	50%	Repetible	
13.1.3	Segregació de xarxes	90%	Definit	
13.2	Transferència d'informació	10%		Mantenir la seguretat de la informació transferida d'una organització a una altre entitat.
13.2.1	Polítiques i procediments de transferència d'informació	10%	Inicial	
13.2.2	Acords sobre la transferència d'informació	10%	Inicial	
13.2.3	Missatgeria electrònica	10%	Inicial	
13.2.4	Acords de confidencialitat o de no divulgació.	10%	Inicial	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
14	SISTEMA D'ADQUISICIÓ,	37%		

	DESENVOLUPAMENT I MANTENIMENT			
14.1	Requisits de seguretat dels sistemes d'informació	50%		Garantir que la seguretat informàtica és una part integral dels sistemes d'informació a través de la totalitat del cicle de vida.
14.1.1	Anàlisi de requisits de seguretat de la informació.	10%	Inicial	
14.1.2	Seguretat dels serveis de les aplicacions en xarxes públiques.	90%	Definit	
14.1.3	Protecció de les transaccions de serveis d'aplicacions	50%	Repetible	
14.2	Seguretat dels processos de desenvolupament i suport	10%		Assegurar que la seguretat d'informació es dissenya i implementa dins el cicle de vida de desenvolupament de sistemes d'informació.
14.2.1	Política de desenvolupament segur	0%	Inexistent	
14.2.2	Procediments de control de canvis del Sistema	10%	Inicial	
14.2.3	Revisió tècnica d'aplicacions després de canvis en la plataforma d'operació	10%	Inicial	
14.2.4	Restriccions als canvis en els paquets de programari	10%	Inicial	
14.2.5	Principis d'enginyeria de sistemes segurs	0%	Inexistent	
14.2.6	Entorn de desenvolupament segur	50%	Repetible	
14.2.7	Desenvolupament externalitzat	0%	Inexistent	
14.2.8	Proves de seguretat dels sistemes	0%	Inexistent	

14.2.9	Proves d’acceptació de sistema	10%	Inicial	
14.3	Dades de prova	50%	Repetible	Garantir la protecció de dades que s'utilitzen per a les proves
14.3.1	Protecció de dades de prova	50%	Repetible	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
15	RELACIONS AMB PROVEÏDORS	12%		
15.1	Seguretat de la informació en les relacions amb els proveïdors	0%		Garantir la protecció dels actius de l'organització que siguin accessibles pels proveïdors.
15.1.1	Política de seguretat de la informació de relacions amb els proveïdors	0%	Inexistent	
15.1.2	Abordar la seguretat dins dels acords amb proveïdors	0%	Inexistent	
15.1.3	Cadena de subministre de la tecnologia d'informació i les comunicacions	0%	Inexistent	
15.2	Gestió de la prestació de serveis de proveïdors	25%		Mantenir uns acords de seguretat de la informació i la prestació de serveis en línia amb els acords amb proveïdors.
15.2.1	Seguiment i revisió dels serveis de proveïdors	50%	Repetible	
15.2.2	Gestió de canvis en els serveis de proveïdors	0%	Inexistent	

SECCIÓ	CONTROL	ESTAT	DESCRIPCIÓ

16	GESTIÓ D'INCIDENTS DE SEGURETAT D'INFORMACIÓ	10%		
16.1	Gestió dels incidents de seguretat de la informació i millores	10%		Garantir un enfocament coherent i eficaç per a la gestió d'incidents de seguretat de la informació, incloent-hi la comunicació d'esdeveniments i debilitats de seguretat.
16.1.1	Responsabilitats i procediments	10%	Inicial	
16.1.2	Informes esdeveniments de seguretat de la informació	10%	Inicial	
16.1.3	Informes de debilitats de seguretat d'informació	10%	Inicial	
16.1.4	L'avaluació dels esdeveniments de seguretat d'informació i les decisions	10%	Inicial	
16.1.5	Resposta a incidents de seguretat d'informació	10%	Inicial	
16.1.6	Aprenentatge obtingut dels incidents de seguretat de la informació	10%	Inicial	
16.1.7	Recopilació de proves	10%	Inicial	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
17	ASPECTES DE SEGURETAT D'INFORMACIÓ DE GESTIÓ DE LA CONTINUITAT DEL NEGOCI	9%		
17.1	Continuïtat seguretat de la informació	7%		La continuïtat seguretat de la informació ha de formar part dels sistemes de gestió de continuïtat de negoci de l'organització.

17.1.1	Planificació de la continuïtat de la seguretat de la informació	10%	Inicial	
17.1.2	Implementació de la continuïtat de la seguretat de la informació	10%	Inicial	
17.1.3	Verificar, revisar i avaluar la continuïtat de la seguretat de la informació	0%	Inexistent	
17.2	Redundàncies	10%		Assegurar la disponibilitat de les instal·lacions de processament d'informació.
17.2.1	Disponibilitat d'instal·lacions de processament d'informació	10%	Inicial	

SECCIÓ	CONTROL	ESTAT		DESCRIPCIÓ
18	COMPLIMENT	28%		
18.1	Compliment dels requisits legals i contractuals	56%		Evitar l'incompliment de les obligacions legals, estatutàries, reglamentàries o contractuals relacionades amb la seguretat de la informació i de qualsevol requisit de seguretat.
18.1.1	Identificació de la legislació aplicable i els requisits contractuals	90%	Definit	
18.1.2	Drets de propietat intel·lectual	50%	Repetible	
18.1.3	Control i protecció de registres	50%	Repetible	
18.1.4	Privacitat i protecció de dades personals	90%	Definit	
18.1.5	Regulació de controls criptogràfics	0%	Inexistent	

18.2	Revisions de la seguretat de la informació	0%		Garantir que la seguretat informàtica és implementada i operada d'acord amb les polítiques i procediments de l'organització.
18.2.1	Revisió independent de la seguretat de la informació	0%	Inexistent	
18.2.2	Acompliment de les polítiques i normes de seguretat	0%	Inexistent	
18.2.3	Revisió de compliment tècnic	0%	Inexistent	

ANNEX II Política de Seguretat

POLÍTICA DE SEGURETAT

Data Publicació	Nom	Firma
04/01/2017	Albert Pintu	

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis
1	**04/01/2017**	Albert Pintu	Aprobat	

1. ENTRADA EN VIGOR

Aquesta Política de Seguretat de la Informació entrarà en vigor l'endemà de la seva publicació en el Butlletí oficial de la UNIF, prèvia aprovació pel Consell de Govern.

2. INTRODUCCIÓ

La UNIVERSITAT FICTÍCIA, d'ara endavant UNIF, depèn dels sistemes TI (Tecnologies d'Informació) per aconseguir els seus objectius institucionals. En conseqüència, aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar a la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

Per això, l'objectiu de la seguretat de la informació és garantir la qualitat de la informació (confidencialitat, integritat, disponibilitat i usos previstos) i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb eficàcia als incidents.

Això implica que l'organització i el seu personal han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, (d'ara 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.

2.1 ASPECTES GENERALS

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, 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 que els diferents actors implicats han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, 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 i serveis han de cerciorar-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 seva

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 a la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC. Així mateix, han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord a l'Article 7 del ENS.

2.2 PREVENCIÓ

Els departaments i serveis 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 han d'implementar les mesures mínimes de seguretat determinades pel 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, documentats i coneguts pels usuaris d'aquests sistemes TIC. Per garantir el compliment d'aquesta política, els departaments i serveis hauran de:

- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent l'impacte que suposin els canvis de configuració realitzats.
- Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

2.3 DETECCIÓ

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, s'han d'establir mecanismes de monitoratge continu de les operacions, per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons l'establert en l'Article 9 del ENS.
El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'Article 8 del ENS. S'establiran mecanismes de detecció, anàlisi i reporti que arribin als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

2.4 RESPOSTA

L'organització ha de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar el punt de contacte per a les comunicacions pel que fa a incidents detectats en àrees de l'entitat o en altres organismes relacionats amb la UNIF.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT) reconeguts a nivell nacional: Iris-CERT, CCNCERT,…

2.5 RECUPERACIÓ

Per garantir la disponibilitat dels serveis crítics, l'organització ha de desenvolupar plans de continuïtat dels sistemes TU com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

3. ABAST

És objecte de la Política de Seguretat plasmar en un document escrit, el conjunt de directrius que regeixen la forma en la qual la Universitat, gestiona i protegeix els recursos d'informació i els sistemes que considera crítics per permetre l'exercici de drets i el compliment de deures per mitjans electrònics en compliment de l'establert en la Llei 11/2007 de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics. Aquesta política s'aplica a tots els sistemes TIC de la Universitat i a totes aquelles persones, institucions, entitats, departaments i serveis que facin ús d'ells, sense excepcions. En aquest sentit, seran considerats sistemes TIC de la Universitat tots aquells sistemes que empren tecnologies de la informació i de les comunicacions per recollir, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre dades i informació.

Per contra, no es considerarà sistema TIC de la Universitat a aquells ordinadors personals finançats a títol individual, no inventariats a nom de la universitat, encara que poguessin ocasionalment ser usats per a labors pròpies de recerca. Per tant queden fora d'aquest àmbit aquests elements. En aquests casos, la Universitat es reserva el dret de proporcionar accés a la xarxa d'aquest tipus de recursos aliens a la mateixa si no es proporcionen uns mínims requisits de seguretat o existeixen indicis o evidències d'un incident potencial de seguretat que pugui comprometre o bé la seguretat de la informació dels sistemes TIC o bé el seu bon nom o imatge corporativa.

4. MISSIÓ

La Universitat Fictícia és una institució pública, dinàmica i innovadora, amb projecció internacional i un campus de referència, la MISSIÓ de la qual és la formació integral dels seus estudiants i el compromís amb l'avanç i la millora de la societat, per mitjà de la creació i transmissió del coneixement i del desenvolupament cultural, científic i tecnològic.

De forma estretament relacionada amb el compliment d'aquesta missió, l'organització desitja manifestar la necessitat d'una infraestructura TIC que prevalgui i fomenti les operatives obertes, enfocades a la funcionalitat, connectivitat i servei a l'usuari, com a funcions prioritàries per a la consecució dels objectius estratègics i institucionals.

5. MARC NORMATIU

Són aplicables les lleis i normatives espanyoles en relació a protecció de dades personals, propietat intel·lectual i ús d'eines telemàtiques.

Aquesta política se situa dins del marc jurídic definit per les lleis i Reials decrets següents:

- Llei Orgànica d'Universitats (6/2001) i Llei Orgànica de modificació de la L.O.O. (4/2007).
- Esquema Nacional de Seguretat (RD 3/2010)
- Llei d'accés electrònic dels ciutadans als serveis públics (11/2007).
- Llei Orgànica de Protecció de Dades (15/1999) i Reglament de desenvolupament de la
- Llei Orgànica (RD 1720/2007)
- Llei de Serveis de la Societat de la Informació (de 12 d'octubre de 2002)

6. ORGANITZACIÓ DE LA SEGURETAT

El manteniment i gestió de la Seguretat dels Sistemes d'Informació depèn íntimament de l'establiment d'una Organització de la Seguretat. Aquesta Organització queda establerta mitjançant la identificació i definició de les diferents activitats i responsabilitats en matèria de gestió de la Seguretat així com de la implantació d'una estructura que les suporti. A

continuació es descriuen les estructures establertes a la Universitat Fictícia amb responsabilitat en diverses àrees relacionades amb la Gestió de la Seguretat de la Informació.

6.1 COMITÈS: FUNCIONS I RESPONSABILITATS

El **Comitè de Seguretat TI** estarà format per:

- El/la Vicerector/a de Tecnologies de la Informació o el/la Vicerector/a competent en la matèria
- Vocal: El/la Secretari/a General
- El/la director/a de l'Àrea de Tecnologies de la Informació
- El/la director/a de l'Àrea de Serveis en Xarxa i Comunicacions
- El/la Cap/a de Àrea de Recursos de la Informació i Serveis en Xarxa
- El/la director/a de el Servei d'Informàtica
- El/la Cap/a de la Divisió de Sistemes del Servei d'Informàtica
- El/la Cap/a de la Divisió d'Aplicacions del Servei d'Informàtica

El Comitè de Seguretat TI nomenarà un secretari o secretària, que tindrà com a funcions les pròpies del càrrec.

El Comitè de Seguretat TI tindrà les següents funcions:

- El Comitè de Seguretat TI informarà al Consell de direcció.
- Divulgació de la política i normativa de seguretat de l'Organització.
- Aprovació de la normativa de seguretat de l'Organització.
- Revisió anual de la política de seguretat.
- Desenvolupament del procediment de designació de rols.
- Designació de rols i responsabilitats.
- Supervisió i aprovació de les tasques de seguiment de l'Esquema Nacional de
- Seguretat:
    - Tasques d'adequació
    - Anàlisi de Riscos
    - Auditoria Biennal

El **Comitè de Protecció de Dades** estarà format per:

- Secretaria General.
- Experts en Protecció de dades.
- Gerència/Vicegerència.
- Un membre del Servei Jurídic.
- Un membre del Servei de Recursos Humans i Organització
- Un membre del Servei d'Informàtica i Comunicacions.
- Un membre del Servei de Recursos Humans i Organització.
- Responsable de seguretat.

La comissió de Protecció de Dades és l'òrgan encarregat del compliment de la legislació vigent en matèria de Protecció de Dades de Caràcter Personal. La seva composició i funcions es detallen a continuació.

El Comitè de Protecció de Dades tindrà les següents funcions:

- Vetllar pel compliment de la normativa de protecció de dades i controlar la seva aplicació, especialment quant als drets d'informació, accés, rectificació, oposició i cancel·lació de dades.
- Impulsar i controlar la implantació de mesures relacionades amb el compliment de la normativa de Protecció de Dades.
- Seguiment del conveni signat amb l'Agència de Protecció de Dades, proposant activitats i millores.
- Avaluació de la situació de la protecció de dades i seguretat informàtica a la Universitat Fictícia, prenent com a referència les recomanacions recollides en els informes de les auditories.
- Proposar recomanacions i accions en matèria de protecció de dades i seguretat informàtica.
- Informar en els seus àmbits d'actuació.
- Col·laborar amb el Comitè de Seguretat TI.

6.2 ROLS: FUNCIONS I RESPONSABILITATS

Responsable dels serveis TI

El/la Vicerector/a de TI tindrà el rol de responsable dels serveis TI de l'Organització.

Tenint per funcions les següents:

- Establiment dels requisits dels serveis TU en matèria de seguretat.
- Treballar en col·laboració amb el/la responsable de seguretat i el/la de sistemes en el manteniment dels sistemes.

Responsable de la informació

El/la Cap/a de Àrea de Recursos de la Informació i Serveis en Xarxa tindrà el rol de responsable de la informació de l'Organització. Tenint per funcions les següents:

Establiment dels requisits de la informació en matèria de seguretat.

Treball en col·laboració amb la persona responsable de seguretat i la persona responsable de sistemes en el manteniment dels sistemes catalogats segons l'Annex I de l'Esquema Nacional de Seguretat.

Responsable de Seguretat

El/la Director/a de el Servei d'Informàtica en el rol de responsable de seguretat de l'Organització. Tenint per funcions les següents:

- Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes TI en el seu àmbit de responsabilitat.
- Realitzar o promoure les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Promoure la formació i conscienciació del Servei d'Informàtica dins del seu àmbit de responsabilitat.
- Coordinar amb els diferents responsables que les mesures de seguretat establertes són adequades per a la protecció de la informació manejada i els serveis prestats.
- Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat del sistema.

- Monitoritzar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria implementats en el sistema.
- Recolzar i supervisar la recerca dels incidents de seguretat des de la seva notificació fins a la seva resolució.
- Aprovació dels procediments de seguretat elaborats pel Responsable del sistema.
- Elaboració de la normativa de seguretat de l'entitat.

Responsable del Sistema TI

Els/les Caps/as de Divisió del Servei d'Informàtica en el rol de responsables del sistema de l'Organització. Tenint per funcions, dins de les seves àrees d'actuació, les següents:

- Desenvolupar, operar i mantenir el sistema durant tot el seu cicle de vida, de les seves especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i política de gestió del sistema establint els criteris d'ús i els serveis disponibles en el mateix.
- Definir la política de connexió o desconnexió d'equips i noves persones usuàries en el sistema.
- Aprovar els canvis que afectin a la seguretat de la manera d'operació del sistema.
- Decidir les mesures de seguretat que aplicaran els subministradors de components del sistema durant les etapes de desenvolupament, instal·lació i prova del mateix.
- Implantar i controlar les mesures específiques de seguretat del sistema i cerciorar-se que aquestes s'integrin adequadament dins del marc general de seguretat.
- Determinar la configuració autoritzada de maquinari i programari a utilitzar en el sistema.
- Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.
- Dur a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema.
- Determinar la categoria del sistema segons el procediment descrit en l'Annex I del ENS i determinar les mesures de seguretat que han d'aplicar-se segons es descriu en l'Annex II del ENS.
- Elaborar i aprovar la documentació de seguretat del sistema.
- Delimitar les responsabilitats de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del sistema.

- Investigar els incidents de seguretat que afectin al sistema, i si escau, comunicació a la persona responsable de seguretat o a qui aquesta determini.
- Establir plans de contingència i emergència, duent a terme freqüents exercicis perquè el personal es familiaritzi amb ells. A més, la persona responsable del sistema 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 poguessin afectar a la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb les persones responsables de la informació afectada, el servei afectat i la persona responsable de seguretat, abans de ser executada.
- Elaboració dels procediments de seguretat necessaris per a l'operativa en el sistema.

Administrador del Sistema

L'Administrador del Sistema és responsable de la implantació, gestió i manteniment de les mesures de seguretat aplicables al Sistema i de la redacció dels Procediments Operatius de Seguretat.
Seran les seves funcions i responsabilitats:

- La implementació, gestió i manteniment de les mesures de seguretat aplicables al Sistema d'Informació.
- La gestió, configuració i actualització, si escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat del Sistema d'Informació.
- La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent el monitoratge que l'activitat desenvolupada en el sistema s'ajusta a l'autoritzat.
- L'aplicació dels Procediments Operatius de Seguretat.
- Aprovar els canvis en la configuració vigent del Sistema d'Informació.
- Assegurar que els controls de seguretat establerts són complerts estrictament.
- Assegurar que són aplicats els procediments aprovats per manejar el sistema d'informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que a tot moment s'ajusten a les autoritzacions pertinents.
- Informar als Responsables de la Seguretat i dels Sistemes d'Informació de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Col·laborar en la recerca i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

6.3. PROCEDIMENT DE DESIGNACIÓ

Concorde als llocs reflectits en la política de seguretat.

6.4. POLÍTICA DE SEGURETAT

Serà missió del Comitè de Seguretat TI la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa. La Política serà aprovada per Consell de Govern i difosa perquè la coneguin totes les parts afectades.

7. DADES DE CARÀCTER PERSONAL

La UNIF realitza tractaments en els quals fa ús de dades de caràcter personal. El Document de Seguretat LOPD de l'Organització es pot trobar en les dependències del Servei d'Informàtica. Aquest document recull els fitxers afectats i les persones responsables corresponents.

Tots els sistemes d'informació de la UNIF s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollits en l'esmentat Document de Seguretat.

8. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada cada dos anys.
- Quan canviï la informació manejada.
- Quan canviïn els serveis prestats.
- Quan ocorri un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat TI establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

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

9. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT

Aquesta Política es desenvoluparà per mitjà de normativa de seguretat que afronti aspectes específics. La normativa de seguretat estarà a la disposició de qualsevol membre de l'organització que necessiti conèixer-la, en particular pels qui utilitzin, operin o administrin els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible en el lloc web de la Universitat.

Aquesta Política de Seguretat de la Informació serà efectiva des del moment de la seva aprovació i fins que sigui reemplaçada per una nova Política.

10. OBLIGACIONS DEL PERSONAL

Totes les persones que formen part de la UNIF tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat desenvolupada a partir d'ella, sent responsabilitat del Comitè de Seguretat TI disposar els mitjans necessaris perquè la informació arribi a les persones o serveis afectats.

S'establirà un programa d'accions de conscienciació contínua per atendre a la totalitat dels i les membres de la UNIF, en particular als qui s'acabin d'incorporar.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TI rebran formació per al maneig segur dels sistemes en la mesura en què la necessitin per realitzar el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

En el cas de detectar-se incompliment de les mesures contemplades en aquesta Política de Seguretat o en les seves normatives de desenvolupament, es podran aplicar mesures preventives i correctores, encaminades a protegir els sistemes TIC.

El procediment i les sancions a aplicar seran les establertes en la legislació sobre règim disciplinari del personal al servei de les Administracions Públiques o de la pròpia UNIF.

11. TERCERES PARTS

Quan la UNIF presti serveis a altres organismes o manegi informació d'altres organismes, se'ls farà partícip d'aquesta Política de Seguretat de la Informació, s'establiran canals per comunicar i coordinar dels respectius Comitès de Seguretat TIC i s'establiran procediments d'actuació per la reacció davant incidents de seguretat.

Quan la UNIF utilitzi serveis de tercers o cedeixi informació a tercers, se'ls exigirà l'ús d'aquesta Política de Seguretat i de la Normativa de Seguretat que concerneixi a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics de comunicació i resolució d'incidències. Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons es defineix en els paràgrafs anteriors, es requerirà al/a la Responsable de Seguretat un informe que precisi 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.

ANNEX I GLOSSARI

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

Autenticitat: Propietat o característica consistent en què una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.

Confidencialitat: Propietat o característica consistent en què la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.

Dades de caràcter personal: Qualsevol informació concernent a persones físiques identificades o identificables. Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

Disponibilitat: Propietat o característica dels actius, consistent en què les entitats o processos autoritzats tenen accés als mateixos quan ho requereixen.

Gestió d'incidents: Pla d'acció per atendre a les incidències que es donin. A més de resoldre-les ha 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.

Integritat: Propietat o característica consistent que l'actiu d'informació no ha estat alterat de manera no autoritzada.

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 que té la potestat d'establir els requisits d'una informació en matèria de seguretat.

Responsable de la seguretat: El responsable de seguretat determinarà 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 destinada a cuidar interessos o satisfer necessitats dels ciutadans.

Sistema d'informació: Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

Sistema TIC: Sistema d'informació que empra tecnologies de la informació i de les comunicacions.

Traçabilitat: Propietat o característica consistent en què les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

ANNEX III Procediment d'Auditoria

PROCEDIMENT D'AUDITORIA

Data Publicació	Nom	Firma
04/01/2017	Albert Pintu	

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis
1	**04/01/2017**	Albert Pintu	Aprobat	

L'objectiu d'aquest procediment es especificar els requeriments, activitats i processos que han de realitzar-se per establir un pla d'auditoria de seguretat de la informació.

1. PLANIFICACIÓ DE L'AUDITORIA

En aquesta primera fase s'establirà la relació entre l'auditor i l'entitat auditada. Es realitzarà un resum de la situació de l'entitat, l'organització, els controls interns, les línies estratègiques, les metodologies empleades, etc, que permetin a l'auditor dissenyar el programa d'auditoria que durà a terme.

El Comitè de Seguretat TI avaluarà propostes de, com a mínim, 3 proveïdors que desenvoluparan el paper d'auditors interns del SGSI de la UNIF. El Comitè TI seleccionarà el proveïdor idoni tenint en compte que el perfil auditor compleixi amb l'experiència, independència i coneixement sobre l'àrea desitjats. L'elecció de l'auditor es realitzarà amb la suficient antelació a l'inici de l'auditoria.

2. EXECUCIÓ DE L'AUDITORIA

La segona fase té per objectiu obtenir i analitzar tota la informació dels processos auditats. La finalitat d'aquesta fase és obtenir l'evidència suficient, competent i rellevant, és a dir, obtenir els elements necessaris per tal que l'auditor pugui establir les conclusions pertinents.

L'execució de l'auditoria interna de la UNIF haurà de seguir els següents processos:

- Reunió inicial.
- Revisió de la documentació per part de l'empresa auditora.
- Planificació i programació d'entrevistes.
- Execució d'auditoria insitu.
- Generació de l'informe final.
- Presentació de resultats.
- Reunió de finalització.

3. INFORME I PLA D'ACCIÓ

La tercera fase constarà del resultat de l'estudi i anàlisi efectuada per l'auditor, el qual de forma normalitzada expressarà la seva opinió per escrit en relació amb els objectius fixats.

Una vegada finalitzada l'auditoria s'haurà de comunicar a les parts interessades i a la direcció o Comitès pertinents els descobriments de la mateixa i generar el pla d'acció relacionat. Aquest pla d'acció haurà de contemplar de manera obligatòria, i sense limitar-se a, les següents característiques:

- Determinació de la causa arrel de les no conformitats.
- Plantejament de les accions correctives i recomanacions.
- Anàlisis de l'eficàcia de les accions correctives d'anteriors auditories.

4. SEGUIMENT

L'organització és la responsable final de resoldre les no conformitats reportades per l'auditoria. Les accions correctives seran planificades en comú acord entre el Comitè de Seguretat TI i l'equip d'auditors. L'organització es fixarà una data límit de 5 mesos per corregir les mesures correctives.

PLANTILLA PLANIFICACIÓ AUDITORIA INTERNA

Objectiu de l'auditoria: _____

Abast: _____

Auditors: _____

Data inici (dd/mm/aaaa): _____Data Finalització (dd/mm/aaaa):_____

Normativa relacionada: _____

Taula d'activitats						
Data	**Hora**	**Lloc**	**Auditor**	**Activitat**	**Documentació relacionada**	**Responsable**

PLANTILLA OBSERVACIONS D'EVIDÈNCIES AUDITORIA INTERNA

Taula d'observacions				
Número	**Observació**	**Norma relacionada**	**Descripció**	**Tipus[4]**

4No conformitat greu, No conformitat lleu, Recomanació

PLANTILLA INFORME ENTRADA

Informe d'entrada
1 Resum revisió anterior
2 Resum executiu d'indicadors
2.1 Auditories realitzades al SGSI
2.2 Efectivitat accions correctores
2.3 Observacions de les auditories
2.4 Accions i resultats de conscienciació
2.5 Incidents atesos
2.6 Aprenentatge

3 Resum executiu d'observacions de l'auditoria
4 Resum executiu de la gestió d'incidents

PLANTILLA INFORME SORTIDA

Informe de sortida
Data (dd/mm/aaaa):
Assistents:
1 Resultats revisió indicadors
1 Resultats revisió indicadors
2 Resultats revisió de la política de seguretat d'informació

3 Resultats revisió abast del SGIS
4 Resultats revisió del nivell de risc acceptable
5 Conclusions

INDICADORS DE SEGURETAT

Data Publicació	Nom	Firma
21/10/2016	Albert Pintu	

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis
1	**21/10/2016**	Albert Pintu	Esborrany	

Descripció dels indicadors implementats:ANNEX V Procediment d'anàlisi i gestió de riscos

Auditories realitzades	
Objectiu	Mesura el percentatge de compliment d'execució de les auditories internes.
Definició	Compliment d'execució de les auditories internes del SGSI.
Responsable	Responsable de Seguretat
Freqüència	Anual
Formula de la mesura	$\left(\frac{Auditories\ realitzades}{Auditories\ programades} \right) \times 100$
Descripció dels valors	Mesura el percentatge de compliment, qualsevol valor diferent a 100% genera una no conformitat.
Valor Objectiu	100%
Llindar	<100%

Formació	
Objectiu	Garantir que tots els empleats han estat formats i conscienciats respecte a la seguretat de la informació.
Definició	Accions formatives dutes a finalment a terme.
Responsable	Àrea de Desenvolupament
Freqüència	Semestral
Formula de la mesura	$\left(\frac{Accions\ de\ Formació\ realitzades}{Accions\ de\ Formació\ programades} \right) \times 100$
Descripció dels valors	Percentatge d'execució de les formacions realitzades al personal respecte a les què inicialment s'havien programat.
Valor Objectiu	100%
Llindar	<80%

Personal assignat	
Objectiu	Seguiment de l'assignació de personal i responsabilitats en matèria de gestió de la seguretat de la informació.
Definició	Aquest indicador determina i fa el seguiment del compromís respecte a la seguretat de la informació pel que fa a la assignació de persones i responsabilitats envers a la seguretat de la informació.
Responsable	Responsable de Seguretat
Freqüència	Anual
Formula de la mesura	$\left(\frac{Número\ persones}{Número\ persones\ any\ anterior} \right) \times 100$
Descripció dels valors	Número de persones amb el corresponent rol de seguretat. Número de persones amb el corresponent rol de seguretat l'any anterior.
Valor Objectiu	80%
Llindar	<60%

Incidències	
Objectiu	Busca destacar aquells incidents reportats que no han estat atesos per els responsables corresponents.
Definició	Mesura el percentatge d'incidents de seguretat de la informació atesos respecte al nombre total d'incidents reportats.
Responsable	Responsable de Seguretat
Freqüència	Semestral
Formula de la mesura	$\left(\frac{Incidents\ atesos}{Incidents\ reportats} \right) \times 100$
Descripció dels valors	Nombre total d'incidents als quals s'han atès i se'ls hi ha donat resposta. Nombre total d'incidents que s'han reportat.

Valor Objectiu	100%
Llindar	<100%

PROCEDIMENT D'ANÀLISI I GESTIÓ DE RISCOS

Data Publicació	Nom	Firma
04/01/2017	Albert Pintu	

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis
1	**04/01/2017**	Albert Pintu	Aprobat	

1. INTRODUCCIÓ

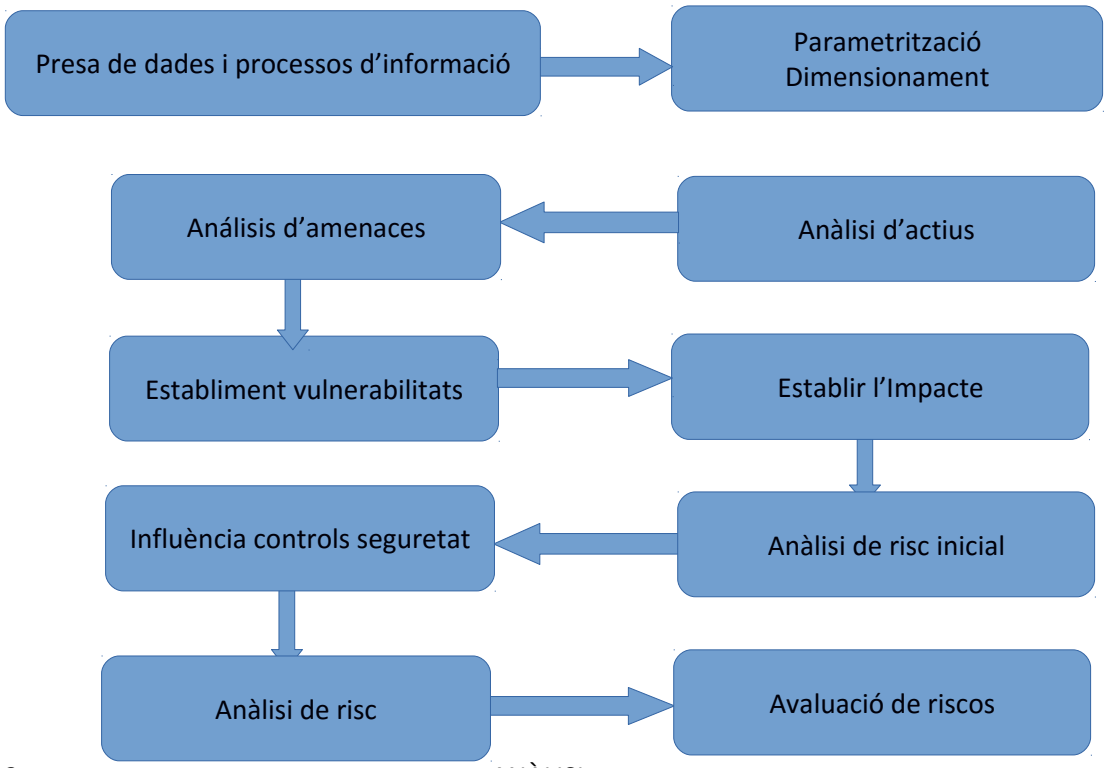
El Procediment d'Anàlisi i Gestió de Riscos establirà la metodologia i les activitats necessàries a realitzar per identificar els riscos a la què està exposada l'organització. Aquest procediment ha de permetre seleccionar les mesures de seguretat que s'han d'implantar adaptades a les necessitats de l'organització i permetre elaborar el pla de contingència de la mateixa.

2. METODOLOGIA

La metodologia aplicada serà Magerit[5]. L'anàlisi de riscos consta essencialment en dos activitats:

- La identificació i valoració d'actius
- La valoració d'amenaces i vulnerabilitats

Mostrem el procés que disposa Magerit per identificar els riscos de l'organització amb el següent flux:



3. ANÀLISI

5La Metodologia MAGERIT, és un mètode formal per investigar els riscos que suporten els Sistemes d'Informació i per recomanar les mesures apropiades que haurien d'adoptar-se per controlar aquests riscos.

3.1 Presa da dades i processos d'informació

Definició de l'abast de l'anàlisi de riscos. S'analitzen els processos crítics de l'organització .

3.2 Parametrització i dimensionament

Els paràmetres s'identifiquen en aquesta fase són els què permeten quantificar els diferents elements utilitzats en l'anàlisi de riscos.

Els paràmetres a quantificar són:

- **Valor dels actius**: És una valoració econòmica de tots els actius que l'organització pretenen analitzar.
- **Vulnerabilitat**: Freqüència d'ocurrència d'una amenaça.

  Vulnerabilitat = freqüència estimada / dies de l'any
- **Impacte**: Pèrdua del valor de l'actiu en el cas que aquest pateixi una incidència. Es Representa en forma de percentatge.
- **Efectivitat del control de seguretat: I**nfluència que tindran les mesures de protecció davant els riscos que detectats.

Taula de valoració d'actius:

Descripció	**Abreviatura**	**Valor**
Molt Alt	MA	100%
Alt	A	75%
Mitjà	M	50%
Baix	B	25%
Mol Baix	MB	10%
Menyspreable	ME	5%

Taula de Freqüència:

Descripció	Abreviatura	Valor
Extremadament freqüent	EF	1
Molt freqüent	MF	0,071
Freqüent	F	0,016
Poc freqüent	PF	0,005
Molt poc freqüent	MPF	0,003
Menyspreable	M	0

Taula d'impacte: Es relaciona la freqüència amb la valoració d'actius.

Risc		**Impacte**					
Freqüència		MA	A	M	B	MB	ME
	EF	MA	MA	MA	MA	MA	A
	MF	MA	MA	A	A	M	M
	F	A	A	M	M	B	B
	PF	M	M	B	B	MB	MB
	MPF	B	B	MB	MB	ME	ME
	M	ME	ME	ME	ME	ME	ME

Representació numèrica:

Risc		Impacte					
		100%	75%	50%	25%	10%	5%
Freqüència	1	100%	75%	50%	25%	10%	5%
	0,071	7,1%	5,3%	3,5%	1,8%	0,7%	0,3%
	0,016	1,6%	1,2%	0,8%	0,4%	0,2%	0,1%
	0,005	0,5%	0,4%	0,25%	0,1%	0,1%	0%
	0,003	0,3%	0,2%	0,1%	0,1%	0%	0%
	0	0%	0%	0%	0%	0%	0%

3.3 Anàlisi d'amenaces

Identifiquen tots els actius disponibles a l'organització i que es troben dins de l'abast definit. Es poden classificar en funció dels valors establerts en el punt anterior.

Es pot agrupar els actius dels sistemes de informació segons:

- Actius físics (hardware).
- Actius lògics (software).
- Actius de personal.
- Actius d'entorn o infraestructura.
- Actius intangibles.

3.4 Anàlisi d'actius

Es classifiquen les amenaces que poden afectar l'organització en quatre grans grups:

- Accidents: Avaries, inundacions, talls de subministrament elèctric, etc.
- Errors: Errors de desenvolupament, de disseny, compatibilitat, actualitzacions, etc.
- Amenaces presencials : Accessos físics no autoritzats, intercepció de la informació, indisponibilitat de recursos, etc.
- Amenaces remotes: Accessos lògics no autoritzats, suplantacions, cucs, etc.

3.5 Establiment vulnerabilitats

S'ha de tenir en comte l'estimació de freqüència d'ocurrència d'una determinada amenaça sobre un actiu de l'organització.

3.6 Establir l'impacte

Es realitza la valoració del impacte que poden provocar les amenaces existents:

- El resultat de l'èxit d'una amenaça respecte un actiu.
- El cost econòmic de les pèrdues produïdes en cada actiu.
- Valoració de les pèrdues quantitatives i qualitatives.
- Agrupació d'impactes en cadena si la pèrdua d'un actiu ho provoca.

3.7 Influència controls de seguretat

El **Risc Intrínsec** és l'anàlisi de la situació en què es troba l'organització en el moment de l'estudi, tingui o no implementades mesures de seguretat. El risc es calculable a partir del valor de l'actiu, la seva vulnerabilitat i l'impacte al que s'exposa.

Risc Intrínsec (o **Inherent**): Valor de l'actiu x Vulnerabilitat x Impacte

3.8 Anàlisi de risc inicial

S'analitzen els controls de seguretat més fonamentals:

- Preventius(redueixen la freqüència, minimitzen les vulnerabilitats).

  (NV: Vulnerabilitat % disminució de la vulnerabilitat, on NV és la nova vulnerabilitat definida)

- Correctius (redueixen l'impacte de l'amenaça).

  (NI: Impacte % disminució de l'Impacte, on NI és el nou impacte definit)

3.9 Anàlisi de risc

S'observarà la reducció del risc aplicant les mesures de seguretat seleccionades anteriorment. En aquest punt es pot calcular el **Risc efectiu**.

El risc efectiu serà el resultat de l'anàlisi que es realitza entre el Risc Intrínsec i les salvaguardies definides per al risc, on s'utilitza la següent fórmula:

Risc efectiu: Valor de l'actiu x Nova vulnerabilitat x Nou Impacte = Valor actiu x (Vulnerabilitat x % disminució de vulnerabilitat) x (Impacte x % disminució d'impacte)

= Risc intrínsec x Percentatge de disminució de vulnerabilitat x Percentatge de disminució d'impacte

3.10 Avaluació de riscos

L'organització ha de decidir quines mesures de seguretat escollir de la llista de controls que acompleixen aquest objectiu. Aquestes mesures es recullen en un pla d'acció el qual contindrà:

- Definició de prioritats. Determinar quins són els riscos més importants.
- Anàlisi cost-benefici de les mesures.
- Selecció dels controls finals.
- Assignació responsabilitats sobre la implantació dels controls.
- Implantar els controls de seguretat designats.

ANNEX VI Declaració d'Aplicabilitat del SGSI

DECLARACIÓ D'APLICABILITAT

Data Publicació	Nom	Firma
04/01/2017	Albert Pintu	

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis
1	**04/01/2017**	Albert Pintu	Aprobat	

La següents taules mostren la declaració d'aplicabilitat del SGSI:

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
5	POLÍTIQUES DE SEGURETAT		
5.1	Direcció de la gestió de seguretat de la informació		
5.1.1	Polítiques de seguretat de la informació	Aplica	La direcció ha reconegut la necessitat de definir, aprovar, publicar i comunicar a empleats i tercers la política per a la seguretat de la informació.
5.1.2	Revisió de les polítiques de seguretat de la informació	Aplica	La direcció reconeix la necessitat d'establiment d'una periodicitat de revisió.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
6	ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ		
6.1	Organització interna		
6.1.1	Rols i responsabilitats de seguretat de la informació	Aplica	En procés. Rols definits i assignats parcialment.
6.1.2	Separació de funcions	Aplica	En procés. Definit i en fase d'ajustament.
6.1.3	Contacte amb les autoritats	Aplica	Definit i en aplicació.
6.1.4	Contacte amb els grups d'interès especial	Aplica	Gestionat i en aplicació.
6.1.5	Seguretat de la informació en la gestió de projectes	Aplica	Pendent d'integrar els equips de desenvolupament.
6.2	Dispositius mòbils i teletreball		
6.2.1	Polítiques per dispositius mòbils	Aplica	Pendent de definició.

6.2.2	Teletreball	Aplica	Pendent de proposta.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
7	SEGURETAT DELS RECURSOS HUMANS		
7.1	Amb anterioritat a l'ocupació		
7.1.1	Control de Selecció	Aplica	S'apliquen les condicions habituals de Recursos Humans.
7.1.2	Termes i condicions d'ocupació	Aplica	S'apliquen les condicions habituals de Recursos Humans.
7.2	Durant l'ocupació		
7.2.1	Responsabilitats de gestió i direcció	Aplica	Pendent de definició.
7.2.2	Conscienciació sobre la seguretat de la informació, l'educació i la formació	Aplica	Pendent de proposta.
7.2.3	Procés disciplinari	Aplica	Pendent de definició.
7.3	Terminació i canvi d'ocupació		
7.3.1	Finalització o canvi de les responsabilitats d'ocupació	Aplica	Pendent de definició.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
8	GESTIÓ D'ACTIUS		
8.1	Responsabilitat dels actius		
8.1.1	Inventari d'actius	Aplica	Definit i en aplicació.
8.1.2	Propietat dels actius	Aplica	Definit i en aplicació.
8.1.3	Ús acceptable dels actius	Aplica	Pendent de proposta.

8.1.4	Devolució d'actius	Aplica	Definit però sense aplicar.
8.2	Classificació de la Informació		
8.2.1	Classificació de la informació	Aplica	Pendent de definició.
8.2.2	Etiquetatge de la informació	Aplica	Pendent de definició.
8.2.3	Manipulació dels actius	Aplica	Pendent de definició.
8.3	Gestió dels mitjans físics.		
8.3.1	Gestió de suports extraïbles	Aplica	Pendent de proposta.
8.3.2	Eliminació dels mitjans	Aplica	Pendent de proposta.
8.3.3	Transferència de mitjans físics	Aplica	Pendent de proposta.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
9	CONTROL D'ACCÉS		
9.1	Requisits de negoci de control d'accés		
9.1.1	Política de control d'accés	Aplica	Definit i en aplicació en Active Directory i Novell. Pendent de millores.
9.1.2	L'accés a les xarxes i serveis de xarxa	Aplica	Pendent de proposta definitiva.
9.2	Gestió d'accés dels usuaris		
9.2.1	Registre d'usuaris i baixes	Aplica	Implementat a nivell de IDM
9.2.2	Aprovisionament d'accés als usuaris	Aplica	Implementat parcialment a nivell de IDM
9.2.3	Gestió de drets d'accés privilegiats	Aplica	Implementat a Active Directory i Novell

9.2.4	Gestió de la informació de connexió de secret dels usuaris	Aplica	Implementat a Active Directory i Novell
9.2.5	Revisió dels drets d'accés dels usuaris	Aplica	Implementat a Active Directory i Novell
9.2.6	Eliminació o ajust dels drets d'accés	Aplica	Implementat a Active Directory i Novell
9.3	Responsabilitat dels usuaris		
9.3.1	Ús del control de la informació de connexió secreta	Aplica	Implementat parcialment segons grups d'usuaris a Active Directory i Novell
9.4	Sistema de control i d'accés a les aplicacions		
9.4.1	Restricció d'accés a la informació	Aplica	Implementat a Active Directory i Novell
9.4.2	Procediments de registre segur	Aplica	Pendent de desenvolupament.
9.4.3	Sistema de gestió de contrasenyes	Aplica	Implementat a nivell de IDM. No aplicable a entorns AD i Novell.
9.4.4	Ús dels programes, utilitats privilegiades	Aplica	Pendent de desenvolupament.
9.4.5	Control d'accés al codi font del programa	Aplica	Pendent de proposta.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
10	CRIPTOGRAFIA		
10.1	Controls criptogràfics		
10.1.1	Política sobre l'ús de controls criptogràfics	Aplica	No definida. Actualment són decisions autònomes i descentralitzades.
10.1.2	Gestió de claus	Aplica	Pendent de proposta.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ

11	SEGURETAT FÍSICA I DE L'ENTORN		
11.1	Àrees segures		
11.1.1	Perímetre de seguretat física	Aplica	Implementat i en funcionament.
11.1.2	Controls d'entrada físics	Aplica	Implementat parcialment i en funcionament.
11.1.3	Protecció d'oficines, sales i instal·lacions	Aplica	Definit i pendent de millores ja aprovades.
11.1.4	Protecció contra amenaces externes i ambientals	Aplica	Pendent de proposta per re-avaluar necessitats.
11.1.5	Treball en àrees segures	Aplica	Pendent de proposta per re-avaluar necessitats.
11.1.6	Lliurament i càrrega de les zones	Aplica	Pendent de proposta.
11.2	Equips		
11.2.1	Ubicació i protecció dels equips	Aplica	Implementat i en funcionament.
11.2.2	Serveis de subministrament	Aplica	Implementat i en funcionament.
11.2.3	La seguretat de cablejat	Aplica	Implementat i en funcionament.
11.2.4	El manteniment de l'equip	Aplica	Implementat i en funcionament. Existeixen excepcions.
11.2.5	Retirada dels actius	Aplica	Pendent de proposta.
11.2.6	Seguretat dels equips i actius fora de les instal·lacions	Aplica	Pendent de proposta.
11.2.7	L'eliminació segura o la reutilització dels equips	Aplica	Pendent de proposta.
11.2.8	Equip d'usuari desatès	Aplica	Pendent de proposta.
11.2.9	Netejar l'escriptori i la política de pantalla	Aplica	Pendent de proposta.

	transparent		

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
12	OPERACIONS DE SEGURETAT		
12.1	Procediments i responsabilitats operacionals		
12.1.1	Procediments operacionals documentats	Aplica	Implementat i en funcionament al 50%
12.1.2	Gestió de canvis	Aplica	Implementat però pendent de millora
12.1.3	Gestió de la capacitat	Aplica	Implementat però pendent de millora
12.1.4	Separació entorns de desenvolupament, prova i operacions	Aplica	Implementat i en funcionament.
12.2	Protecció contra el codi maliciós		
12.2.1	Controls contra el codi maliciós.	Aplica	Implementat però pendent de millora (nous tallafocs, nou software antivirus)
12.3	Còpia de seguretat		
12.3.1	Informació de còpia de seguretat	Aplica	Implementat i en funcionament.
12.4	Registre i supervisió		
12.4.1	Registre d'esdeveniments	Aplica	Implementat i en funcionament.
12.4.2	Protecció de la informació de registre	Aplica	Implementat però pendent de millora
12.4.3	Administrador i operador registres	Aplica	Implementat però pendent de millora
12.4.4	Sincronització del rellotge	Aplica	Implementat i en funcionament.
12.5	Control de programari operacional		

12.5.1	Instal·lació de programari en sistemes operatius	Aplica	Implementat i en funcionament.
12.6	Gestió tècnica de vulnerabilitats		
12.6.1	Gestió de vulnerabilitats tècniques	Aplica	Pendent de proposta.
12.6.2	Restriccions en la instal·lació del programari	Aplica	Pendent de proposta.
12.7	Sistemes d'informació consideracions d'auditoria		
12.7.1	Sistemes d'informació controls d'auditoria	Aplica	Pendent de proposta.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
13	SEGURETAT DE LES COMUNICACIONS		
13.1	Gestió de seguretat de xarxa		
13.1.1	Controls de xarxa	Aplica	Es disposa de tallafocs de capa 3 i proxy parcialment.
13.1.2	Seguretat dels serveis de xarxa	Aplica	Es disposa de tallafocs de capa 3 i proxy parcialment.
13.1.3	Segregació de xarxes	Aplica	Implementat i en funcionament.
13.2	Transferència d'informació		
13.2.1	Polítiques i procediments de transferència d'informació	Aplica	Pendent de proposta.
13.2.2	Acords sobre la transferència d'informació	Aplica	Pendent de proposta.
13.2.3	Missatgeria electrònica	Aplica	Implementat i en funcionament.

13.2.4	Acords de confidencialitat o de no divulgació.	Aplica	Implementat i en funcionament (segons unitat o departament).

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
14	SISTEMA D'ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT		
14.1	Requisits de seguretat dels sistemes d'informació		
14.1.1	Anàlisi de requisits de seguretat de la informació.	Aplica	Pendent de proposta.
14.1.2	Seguretat dels serveis de les aplicacions en xarxes públiques.	Aplica	Pendent de definició.
14.1.3	Protecció de les transaccions de serveis d'aplicacions	Aplica	Pendent de proposta.
14.2	Seguretat dels processos de desenvolupament i suport		
14.2.1	Política de desenvolupament segur	Aplica	Pendent de proposta.
14.2.2	Procediments de control de canvis del Sistema	Aplica	No hi ha un estàndard. Solucions individuals segons l'equip.
14.2.3	Revisió tècnica d'aplicacions després de canvis en la plataforma d'operació	Aplica	Pendent de desenvolupar.
14.2.4	Restriccions als canvis en els paquets de programari	Aplica	Pendent de desenvolupar.
14.2.5	Principis d'enginyeria de sistemes segurs	Aplica	Pendent de desenvolupar.
14.2.6	Entorn de desenvolupament segur	Aplica	Parcialment, segons l'equip de desenvolupament.
14.2.7	Desenvolupament externalitzat	Aplica	Parcialment, segons l'equip de desenvolupament.

14.2.8	Proves de seguretat dels sistemes	Aplica	Pendent de desenvolupar.
14.2.9	Proves d'acceptació de sistema	Aplica	Parcialment, segons l'equip de desenvolupament.
14.3	Dades de prova		
14.3.1	Protecció de dades de prova	Aplica	Pendent de desenvolupar.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
15	RELACIONS AMB PROVEÏDORS		
15.1	Seguretat de la informació en les relacions amb els proveïdors		
15.1.1	Política de seguretat de la informació de relacions amb els proveïdors	Aplica	En procés. Juntament amb l'aprovació de la política de seguretat.
15.1.2	Abordar la seguretat dins dels acords amb proveïdors	Aplica	En procés. Juntament amb l'aprovació de la política de seguretat.
15.1.3	Cadena de subministre de la tecnologia d'informació i les comunicacions	Aplica	Pendent de desenvolupar.
15.2	Gestió de la prestació de serveis de proveïdors		
15.2.1	Seguiment i revisió dels serveis de proveïdors	Aplica	Pendent de desenvolupar. Accions individuals fora de l'espectre del SGSI.
15.2.2	Gestió de canvis en els serveis de proveïdors	Aplica	Pendent de desenvolupar.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
16	GESTIÓ D'INCIDENTS DE SEGURETAT D'INFORMACIÓ		

16.1	Gestió dels incidents de seguretat de la informació i millores		
16.1.1	Responsabilitats i procediments	Aplica	En desenvolupament.
16.1.2	Informes esdeveniments de seguretat de la informació	Aplica	Implementat i en funcionament.
16.1.3	Informes de debilitats de seguretat d'informació	Aplica	Pendent unificar fonts externes.
16.1.4	L'avaluació dels esdeveniments de seguretat d'informació i les decisions	Aplica	Pendent de desenvolupar.
16.1.5	Resposta a incidents de seguretat d'informació	Aplica	Pendent de desenvolupar.
16.1.6	Aprenentatge obtingut dels incidents de seguretat de la informació	Aplica	Pendent de desenvolupar.
16.1.7	Recopilació de proves	Aplica	Pendent de desenvolupar.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
17	ASPECTES DE SEGURETAT D'INFORMACIÓ DE GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI		
17.1	Continuïtat seguretat de la informació		
17.1.1	Planificació de la continuïtat de la seguretat de la informació	Aplica	Documentat i parcialment executat.
17.1.2	Implementació de la continuïtat de la seguretat de la informació	Aplica	Documentat i parcialment executat.
17.1.3	Verificar, revisar i avaluar la continuïtat de	Aplica	Documentat i parcialment executat.

	la seguretat de la informació		
17.2	Redundàncies		
17.2.1	Disponibilitat d'instal·lacions de processament d'informació	Aplica	Pendent externalització parcial de serveis.

SECCIÓ	CONTROL	APLICA	JUSTIFICACIÓ
18	COMPLIMENT		
18.1	Compliment dels requisits legals i contractuals		
18.1.1	Identificació de la legislació aplicable i els requisits contractuals	Aplica	Definit i en funcionament.
18.1.2	Drets de propietat intel·lectual	Aplica	En Procés.
18.1.3	Control i protecció de registres	Aplica	En Procés. Pendent accions de millora.
18.1.4	Privacitat i protecció de dades personals	Aplica	Definit, implementat i en funcionament.
18.1.5	Regulació de controls criptogràfics	Aplica	Pendent de desenvolupar.
18.2	Revisions de la seguretat de la informació		
18.2.1	Revisió independent de la seguretat de la informació	Aplica	Pendent de desenvolupar.
18.2.2	Acompliment de les polítiques i normes de seguretat	Aplica	Pendent de desenvolupar.
18.2.3	Revisió de compliment tècnic	Aplica	Pendent de desenvolupar.

ANNEX VII Valoració d'actius

CODI	ACTIU	VALOR
I.1	Centre de Càlcul 1 (CPD)	100000
I.2	Centre de Càlcul 2 (CPD)	100000
I.3	Centre de Càlcul 3 (CPD)	60000
I.4	Arxiu.	100000
I.5	RITI 1. (Recinte d'instal·lacions de Telecomunicacions)	40000
I.6	RITI 2.	40000
I.7	RITI 3.	40000
H.1	Workstations	24000000
H.2	Portàtils	400000
H.3	Tablets	20000
H.4	Mòbils	20000
H.5	Impressores	20000
H.6	Routers	20000
H.7	Switchs	250000
H.8	Tallafocs	200000
H.9	Balancejadors de càrrega	50000
H.10	Proxys	20000
H.11	Cabines de disc	300000
H.12	Cluster VMWARE	60000
H.13	Cluster ORACLE	40000
H.14	Centraleta telefonia IP	20000
H.15	SIEM	50000
H.16	IDS/IPS	10000
H.17	Controladores WiFi + Acces Points	100000
A.1	Sistemes operatius clients (Windows, Linux, MacOS)	50000
A.2	Windows Server 2012R2	30000
A.3	SUSE Enterprise	30000

A.4	Solaris	20000
A.5	Apache Tomcat	10000
A.6	Weblogic	20000
A.7	Antivirus	150000
A.8	Offimàtica	150000
A.9	Oracle Database	100000
A.10	Software gestió backups (Coomvault, VEEM)	20000
A.11	Software Gestió Acadèmic	50000
A.12	OpenCMS/Liferay Portal/Intranet	60000
A.13	Novell	30000
A.14	VMWARE	10000
D.1	Backup	100000
D.2	Dades RRHH	50000
D.3	Documentum	100000
D.4	Dades alumnes	50000
D.5	Correu i eines de col·laboració (al núvol)	50000
X.1	Connexions primàries fibra amb anella científica	50000
X.2	Connexió secundària fibra amb anella científica	15000
X.3	Routers/Switch	300000
X.4	Xarxa wifu: Controladores + Acces Points	100000
S.1	Impressió	50000
S.2	Web	100000
S.3	Correu + eines col·laboratives	100000
S.4	Formació	50000
AUX.1	Armaris racks CPDs	20000
AUX.2	Sistema climàtic CPD	200000
AUX.3	Sistemes d'alimentació continua i secundària	150000
AUX.4	Cablejat elèctric	100000
AUX.5	Cablejat xarxa	30000

AUX.6	Sistema antiincendis	100000
P.1	Responsable del departament TI	75000
P.2	Responsable de seguretat	60000
P.3	Desenvolupadors	800000
P.4	Personal de sistemes i comunicacions	500000

ANNEX VIII Dimensions de Seguretat

Llegenda:

A: Autenticitat, C: Confidencialitat, I: Integritat, D: Disponibilitat, T: Traçabilitat

CODI	ACTIU	VALOR	ASPECTES CRÍTICS				
			A	C	I	D	T
I.1	Centre de Càlcul 1 (CPD)	**10**	8	6	9	9	8
I.2	Centre de Càlcul 2 (CPD)	**10**	8	6	9	9	8
I.3	Centre de Càlcul 3 (CPD)	**10**	8	6	9	9	8
I.4	Arxiu.	**9**	8	6	9	9	8
I.5	RITI 1. (Recinte d'instal·lacions de	**9**	7	6	9	9	8
I.6	RITI 2.	**9**	7	6	8	9	8
I.7	RITI 3.	**9**	7	6	8	9	8
H.1	Workstations	**6**	6	5	6	5	5
H.2	Portàtils	**6**	6	5	6	5	5
H.3	Tablets	**5**	5	5	5	3	3
H.4	Mòbils	**5**	4	6	6	6	6
H.5	Impressores	**3**	2	2	4	5	5
H.6	Routers	**6**	5	6	8	8	6
H.7	Switchs	**6**	5	6	8	8	6
H.8	Tallafocs	**7**	7	6	8	9	8
H.9	Balancejadors de càrrega	**7**	6	4	8	8	5
H.10	Proxys	**6**	6	5	6	5	6
H.11	Cabines de disc	**10**	9	9	10	10	8
H.12	Cluster VMWARE	**8**	8	8	9	9	8
H.13	Cluster ORACLE	**8**	9	9	10	10	8
H.14	Centraleta telefonia IP	**7**	3	6	6	9	8
H.15	SIEM	**5**	6	5	6	5	5
H.16	IDS/IPS	**6**	6	5	6	5	5
H.17	Controladores WiFi + Acces Points	**4**	2	3	2	3	3

A.1	Linux, MacOS)	**5**	5	6	6	5	5
A.2	Windows Server 2012R2	**5**	5	6	6	5	5
A.3	SUSE Enterprise	**5**	5	6	6	5	5
A.4	Solaris	**5**	5	6	6	5	5
A.5	Apache Tomcat	**5**	5	6	6	5	5
A.6	Weblogic	**5**	5	6	6	5	5
A.7	Antivirus	**5**	5	6	6	5	5
A.8	Offimàtica	**4**	2	3	2	3	3
A.9	Oracle Database	**7**	6	7	6	6	7
A.10	Software gestió backups (Coomvault,	**6**	5	6	5	5	6
A.11	Software Gestió Acadèmic	**8**	9	10	10	9	6
A.12	OpenCMS/Liferay Portal/Intranet	**6**	5	6	5	5	6
A.13	Novell	**5**	5	6	6	5	5
A.14	VMWARE	**5**	5	6	6	5	5
D.1	Backup	**9**	9	9	9	10	7
D.2	Dades RRHH	**8**	9	10	10	9	6
D.3	Documentum	**8**	9	10	10	9	6
D.4	Dades alumnes	**8**	9	10	10	9	6
D.5	Correu i eines de col·laboració (al	**8**	8	9	9	9	9
X.1	Connexions primàries fibra amb anella	**6**	5	6	8	8	6
X.2	Connexió secundària fibra amb anella	**6**	5	6	8	8	6
X.3	Routers/Switch	**6**	5	6	8	8	6
X.4	Xarxa wifu: Controladores + Acces	**6**	5	6	8	8	6
S.1	Impressió	**5**	5	6	6	5	5
S.2	Web	**8**	8	9	9	9	9
S.3	Correu + eines col·laboratives	**8**	8	9	9	9	9
S.4	Formació	**3**	3	3	3	3	3
AUX.1	Armaris racks CPDs	**5**				6	
AUX.2	Sistema climàtic CPD	**6**				9	

AUX.3	Sistemes d'alimentació continua i	**5**	9
AUX.4	Cablejat elèctric	**7**	9
AUX.5	Cablejat xarxa	**7**	9
AUX.6	Sistema antiincendis	**5**	9
P.1	Responsable del departament TI	**8**	6
P.2	Responsable de seguretat	**8**	6
P.3	Desenvolupadors	**8**	6
P.4	Personal de sistemes i comunicacions	**8**	6

ANNEX IX Impacte Potencial (Valoració econòmica)

CODI	ACTIU	VALOR QUANTITATIU	IMPACTE	IMPACTE POTENCIAL
I.1	Centre de Càlcul 1 (CPD)	100000	**1**	**100000**
I.2	Centre de Càlcul 2 (CPD)	100000	**1**	**100000**
I.3	Centre de Càlcul 3 (CPD)	60000	**1**	**60000**
I.4	Arxiu.	100000	**0,75**	**75000**
I.5	RITI 1. (Recinte d'instal·lacions de	40000	**0,75**	**30000**
I.6	RITI 2.	40000	**0,75**	**30000**
I.7	RITI 3.	40000	**0,75**	**30000**
H.1	Workstations	24000000	**0,5**	**12000000**
H.2	Portàtils	400000	**0,5**	**200000**
H.3	Tablets	20000	**0,5**	**10000**
H.4	Mòbils	20000	**0,5**	**10000**
H.5	Impressores	20000	**0,25**	**10000**
H.6	Routers	20000	**0,5**	**10000**
H.7	Switchs	250000	**0,5**	**125000**
H.8	Tallafocs	200000	**0,75**	**150000**
H.9	Balancejadors de càrrega	50000	**0,75**	**37500**
H.10	Proxys	20000	**0,5**	**10000**
H.11	Cabines de disc	300000	**1**	**300000**
H.12	Cluster VMWARE	60000	**0,75**	**45000**
H.13	Cluster ORACLE	40000	**0,75**	**30000**
H.14	Centraleta telefonia IP	20000	**0,75**	**15000**
H.15	SIEM	50000	**0,5**	**25000**
H.16	IDS/IPS	10000	**0,5**	**5000**
H.17	Controladores WiFi + Acces Points	100000	**0,5**	**50000**
A.1	Linux, MacOS)	50000	**0,5**	**25000**

A.2	Windows Server 2012R2	30000	**0,5**	**15000**
A.3	SUSE Enterprise	30000	**0,5**	**15000**
A.4	Solaris	20000	**0,5**	**10000**
A.5	Apache Tomcat	10000	**0,5**	**5000**
A.6	Weblogic	20000	**0,5**	**10000**
A.7	Antivirus	150000	**0,5**	**75000**
A.8	Offimàtica	150000	**0,5**	**75000**
A.9	Oracle Database	100000	**0,75**	**75000**
A.10	Software gestió backups (Coomvault,	20000	**0,5**	**10000**
A.11	Software Gestió Acadèmic	50000	**0,75**	**37500**
A.12	OpenCMS/Liferay Portal/Intranet	60000	**0,5**	**30000**
A.13	Novell	30000	**0,5**	**15000**
A.14	VMWARE	10000	**0,5**	**5000**
D.1	Backup	100000	**0,75**	**75000**
D.2	Dades RRHH	50000	**0,75**	**37500**
D.3	Documentum	100000	**0,75**	**75000**
D.4	Dades alumnes	50000	**0,75**	**37500**
D.5	Correu i eines de col·laboració (al	50000	**0,75**	**37500**
X.1	Connexions primàries fibra amb	50000	**0,5**	**25000**
X.2	Connexió secundària fibra amb anella	15000	**0,5**	**7500**
X.3	Routers/Switch	300000	**0,5**	**150000**
X.4	Xarxa wifu: Controladores + Acces	100000	**0,5**	**50000**
S.1	Impressió	50000	**0,5**	**25000**
S.2	Web	100000	**0,75**	**75000**
S.3	Correu + eines col·laboratives	100000	**0,75**	**75000**
S.4	Formació	50000	**0,25**	**12500**
AUX.1	Armaris racks CPDs	20000	**0,5**	**10000**
AUX.2	Sistema climàtic CPD	200000	**0,5**	**100000**
AUX.3	Sistemes d'alimentació continua i	150000	**0,5**	**75000**

AUX.4	Cablejat elèctric	100000	**0,75**	**75000**
AUX.5	Cablejat xarxa	30000	**0,75**	**22500**
AUX.6	Sistema antiincendis	100000	**0,5**	**50000**
P.1	Responsable del departament TI	75000	**0,75**	**56250**
P.2	Responsable de seguretat	60000	**0,75**	**45000**
P.3	Desenvolupadors	800000	**0,75**	**600000**
P.4	Personal de sistemes i comunicacions	500000	**0,75**	**375000**

ANNEX X Anàlisi d'Amenaces

Llegenda:

I : Instal·lacions, H : Hardware, A : Aplicacions, D : Dades, X : Xarxa, S : Serveis,

AUX : Equipament Auxiliar, P : Personal

CATEGORIA	AMENAÇA	ACTIU							
		I	H	A	D	X	S	AUX	P
Amenaces d'origen natural	Incendi	X	X			X		X	
	Inundació	X	X					X	
	Desastre natural	X	X					X	
Amenaces d'entorn o d'origen industrial	Foc i danys per aigua	X	X					X	
	Degradació de suports i equipament	X	X	X					
	Avaria climatització (temperatura i humitat)	X	X					X	
	Fallada subministrament elèctric	X	X			X		X	
	Contaminació i emanació electromagnètica		X	X		X			
	Manipulació d'equipament		X	X					
	Avaria física	X	X			X		X	
	Avaria lògica			X	X		X		
	Interrupció d'altres serveis i subministres essencials	X	X					X	
	Fallada servei de comunicacions					X			
Errors i fallades no intencionades	Error de configuració		X	X					
	Errors de manteniment programari			X	X				

	Errors de manteniment hardware		X						
	Errors dels administradors		X	X		X	X		
	Errors humans (usuaris)	X	X	X	X	X	X	X	X
	Pèrdua o fuga d'informació				X				
	Vulnerabilitats de programari			X	X				
	Indisponibilitat de personal								X
	Caigudes per esgotament de recursos		X			X	X		
Atacs intencionats	Destrucció d'informació no autoritzada				X				X
	Robatori		X		X				X
	Atac informàtic		X	X	X	X	X		X
	Coacció				X				X
	Manipulació de registres i logs			X	X				X
	Enginyeria Social				X				X
	Denegació de servei				X		X		X
	Accés no autoritzat a sistemes		X	X	X				X
	Manipulació de programes			X	X				X
	Manipulació d'equips		X		X				X
	Divulgació no autoritzada				X				X
	Abús de privilegis			X	X				X
	Suplantació d'identitat			X	X				X
	Ús no previst			X	X				X

ANNEX XI Informe d'auditoria

INFORME D'AUDITORIA

Data Publicació	Nom	Firma
16/12/2016	Albert Pintu	

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis
1	**16/12/2016**	Albert Pintu	Esborrany	

1. Objectiu

Identificar el nivell de cumpliment del SGSI de la UNIF respecte als controls i clausules de la norma internacional ISO 27002.

La ISO 27002 analitza la seguretat de la informació d'una organització, sigui del tipus que sigui i independentment de les seves dimensions. La ISO s'agrupa amb 114 controls o mesures preventives , organitzades en 14 àrees i 35 objectius.

El resultat de l'auditoria estableix l'estat de seguretat d'una organització en un moment donat del temps en tots els àmbits de protecció: físic, lògic, organitzatiu i legal.

2. Identificació del beneficiari

UNIF, Universitat Ficticia de Catalunya

Adreça: Passeig de les universitats, núm 1.

NIF: xxxxxxxxxx

Persona de contacte: Nom Cognom1 Cognom2

3. Abast

L'abast de l'auditoria estarà marcat per la Declaració d'Aplicabilitat del SGSI

4. Equip Auditor

L'auditoria fou executada per Albert Pintu Pla.

5. Dates d'execució de l'Auditoria

Aquesta realitzada entre el XX de desembre de 2016 i el YY de gener de 2017.

Les tasques realitzades han estat:

- Recull de dades i informació.
- Realització de qüestionaris.
- Visites a les instal·lacions.
- Realització de proves d'àmbit tècnic.

- Estudi i anàlisi de la informació recollida.
- Elaboració informe de No conformitats.

6. Lloc

L'auditoria es va executar a les instal·lacions de la UNIF, incloent els centres de processament de dades i espais necessaris per l'execució de la mateixa.

7. Normativa

La normativa utilitzada per du a terme l'auditoria es basa en els 114 controls o mesures preventives organitzades en 14 àrees i 35 objectius de control de la i ISO/IEC 27002. Aquests controls ens permetran conèixer l'estat actual de la Organització en relació a la Seguretat de la Informació.

La valoració es realitzarà segons el model de maduresa de la capacitat (CMM). La següent taula mostra els barems utilitzats:

MADURESA (CMM)	EFECTIVITAT	DESCRIPCIÓ
Inexistent	0 %	Carència completa de qualsevol procés que reconeguem.
Inicial	10%	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal.
Reproduïble, però intuïtiu	50%	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca.
Procés definit	90%	La organització sencera participa al procés.
Gestionat y mesurable	95%	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.
Optimitzat	100%	Els processos estan sota constant millora.

8. Informe detallat

Anàlisi dels controls:

ÀREA	5. Polítiques de la Seguretat de la Informació				
Control ISO/IEC 27002:2013: 5.1 Direcció de gestió de seguretat de la informació					
Proporcionar orientació i suport a la seguretat de la informació d'acord amb els requeriments del negoci, les lleis i reglaments pertinents de gestió.					
Treball realitzat					
És revisa l'existència d'una política de Seguretat.					
Observació					
Verificació de l'existència d'una política de Seguretat aprovada per l'organització, publicada i comunicada als empleats i col·laboradors externs.					
Evidències					
Document Política de Seguretat. Data publicació: dd/mm/aaaa					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	6.Organització de la seguretat de la informació
Control ISO/IEC 27002:2013: 6.1 Organització interna	
Marc de gestió establert per l'administració de l'aplicació de la seguretat de la informació a l'organització.	
Treball realitzat	
Revisió dels dominis de seguretat establerts per l'administració de l'aplicació de la seguretat de la informació a l'organització.	

Observació					
Verificació que la UNIF disposa dels rols, funcions, procediments necessaris.					
Evidències					
Existència entorn de seguretat documentat.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**6.Organització de la seguretat de la informació**
Control ISO/IEC 27002:2013: 6.2 Els dispositius mòbils i el teletreball	
Garantir la seguretat en el teletreball i en l'ús de dispositius mòbils.	
Treball realitzat	
Revisió polítiques de teletreball. **Revisió polítiques per dispositius mòbils.** **Revisió del servei VPN i els mètodes d'autenticació utilitzats.**	
Observació	
No es facilita una normativa al respecte.	
Evidències	
Existència normativa teletreball, però sense indicacions de seguretat. **Inexistència política per a dispositius mòbils.** **Connexió VPN utilitza RSA_AES_128_SHA1**	
Recomanació	
Modificació normativa de treball indicant procediments, especialment fent referència a l'ús de la VPN.	

Creació normativa per dispositius mòbils (política antivirus, tallafocs, credencials)					
Estat:	**En curs**	**Responsable:**	**RRHH/Informàtica**	**Termini:**	**6 mesos**
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	**7. La seguretat dels recursos humans**				
Control ISO/IEC 27002:2013: 7.1 Amb anterioritat a l'ocupació					
Empleats i terceres empreses entenen les responsabilitats a les que estan sotmeses segons les seves funcions.					
Treball realitzat					
Avaluació de les mesures de seguretat existents abans, durant i després de la contractació, incloent l'existència d'acords de confidencialitat i plans de informació/conscienciació.					
Observació					
Verificació de l'existència d'acords de confidencialitat abans de l'inici d'una contractació externa però no estès a tots els àmbits.					
Evidències					
Existència de procediments de contractació sense acords de confidencialitat.					
Recomanació					
Estendre la comunicació d'acords de confidencialitat i polítiques de seguretat als proveïdors i empreses externes de tots els àmbits.					
Estat:	**En curs**	**Responsable:**	**Gestió patrimonial**	**Termini:**	**6 mesos**
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	**7. La seguretat dels recursos humans**
Control ISO/IEC 27002:2013: 7.2 Durant l'ocupació	
Empleats i terceres empreses entenen les responsabilitats a les que estan sotmeses segons les seves funcions i compleixen els requisits de seguretat.	
Treball realitzat	

Avaluació de mesures de seguretat existents.
Observació
Jornades d'informació i conscienciació impartides.
Evidències
Documents i informació publicada durant les jornades de formació. **Comprovants d'assistència dels empleats.**
Recomanació
El procés disciplinari no referencia les polítiques de seguretat.

Estat:		**Responsable:**		**Termini:**	
CONCLUSIÓ:			**CONFORME**		

ÀREA	**7. La seguretat dels recursos humans**
Control ISO/IEC 27002:2013: 7.3 Terminació i canvi d'ocupació	
Protecció dels interessos de l'organització després de la finalització de la relació contractual.	
Treball realitzat	
Avaluació de les mesures de seguretat posteriors a la finalització de la contractació.	
Observació	
Inexistència de procediment de devolució dels materials (tangibles i intangibles).	
Evidències	
Inexistència del procediment.	
Recomanació	
Implementar procediment de devolució de materials i signatura verificant que el treballador no s'enduu informació.	

Estat:	**En curs**	**Responsable:**	**RRHH**	**Termini:**	**6 mesos**

CONCLUSIÓ:	NO CONFORME

ÀREA	8. Gestió d'actius				
Control ISO/IEC 27002:2013: 8.1 La responsabilitat dels actius					
Identificació dels actius i definició de les responsabilitats de protecció adequades.					
Treball realitzat					
Revisió del inventari dels actius que gestionen o emmagatzemen informació corporativa.					
Observació					
Es consulten diferents actius al atzar i es verifica que estigui definit un responsable/propietari.					
Evidències					
Extracció de la informació referents als actius seleccionats a través de l'aplicació corresponent.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	8. Gestió d'actius
Control ISO/IEC 27002:2013: 8.2 Classificació de la Informació	
Assegurar el nivell adequat de protecció d'acord amb la importància de l'actiu per a l'organització.	
Treball realitzat	
Revisió de la classificació de la informació i de l'establiment de mesures de seguretat per a la gestió de suports.	
Observació	
Observació dels actius identificats amb dades confidencials. Els informes de compliment normatiu mostren	

aquests actius i el seu nivell de protecció.					
Evidències					
Extracció de la informació referents als actius seleccionats a través de l'aplicació corresponent.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**8. Gestió d'actius**
Control ISO/IEC 27002:2013: 8.3 Gestió de mitjans físics	
Evitar la divulgació no autoritzada, modificació, eliminació o destrucció de la informació emmagatzemada en els mitjans.	
Treball realitzat	
Revisió dels permisos de modificació, creació i eliminació dels propietaris de cada actiu.	
Observació	
Es consulten diferents actius al atzar i es verifica que estigui definit un responsable/propietari.	
Evidències	
Extracció de la informació referents als actius seleccionats a través de l'aplicació corresponent.	
Recomanació	
No aplica	

Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	9. Control d'accés				
Control ISO/IEC 27002:2013: 9.1 Els requisits de negoci de control d'accés					
Control d'accés a les instal·lacions de processament d'informació.					
Treball realitzat					
Revisió del procediment d'accés de visites i personal extern. Comprovació del registre d'entrades i sortides. Avaluació del mètode d'accés.					
Observació					
En els diferents Campus/edificis es detecta que espot accedir per diferents zones sense identificació oportuna. **L'accés als CPD es realitza utilitzant una targeta identificadora de proximitat al personal autoritzat.**					
Evidències					
Procediment d'accés de personal extern als CPD. Registre d'entrada als CPDs de la tarja de proximitat.					
Recomanació					
Ampliar l'accés als espais amb ús obligatori de la tarja de proximitat.					
Estat:	**En curs**	**Responsable:**	**Manteniment / Informàtica**	**Termini:**	**1 any**
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	9. Control d'accés
Control ISO/IEC 27002:2013: 9.2 Gestió d'accés dels usuaris	
Evitar l'accés no autoritzat als sistemes i serveis.	
Treball realitzat	
Comprovació de la gestió d'altes i baixes d'usuaris a traves del IDM i del AD/Novell.	
Observació	
Es comproven els accessos als sistemes a través dels logs generats.	
Evidències	

Procediment de gestió d'altes i baixes al IDM.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**9. Control d'accés**				
Control ISO/IEC 27002:2013: 9.3 Responsabilitat dels usuaris					
Els usuaris s'han de responsabilitzar de salvaguardar la informació d'accés.					
Treball realitzat					
Es verifica la gestió d'usuaris privilegiats a través dels protocols establerts.					
Observació					
Es comproven els accessos als sistemes a través dels logs generats al software d'auditoria.					
Evidències					
Procediment de gestió d'altes i baixes al IDM. **Logs generats al sistema d'auditoria de fitxers.**					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**9. Control d'accés**

Control ISO/IEC 27002:2013: 9.4 Sistema de control i d'accés a les aplicacions					
Prevenció dels accessos no autoritzats als sistemes i aplicacions.					
Treball realitzat					
Revisió dels events generats als logs del IDM, AD i Novell. **Logs generats al sistema d'auditoria de fitxers.**					
Observació					
Verificació dels controls d'accessos als sistemes a través de la comprovació dels logs generats.					
Evidències					
Gestió d'alertes i logs.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**10 Criptografia**
Control ISO/IEC 27002:2013: 10.1 Controls criptogràfics	
Utilització de la criptografia per protegir la confidencialitat, autenticitat i integritat de la informació.	
Treball realitzat	
Realització de controls bàsics sobre certificats digitals i claus criptogràfiques (comprovació de certificats autosignats).	
Observació	
Es comprova que existeix una política definida d'ús de la cadena de certificats proporcionada per DigiCert. **Es comprova l'existència de certificats autosignats en alguns serveis.**	
Evidències	

Document amb llista de persones autoritzades a sol·licitar i aprovar els certificats digitals corporatius. **Llistat dels certificats digitals vigents.**					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**11.La Seguretat física i de l'entorn**				
Control ISO/IEC 27002:2013: 11.1 Les àrees segures					
Prevenir l'accés físic no autoritzat, els danys i les interferències a les instal·lacions de processament d'informació.					
Treball realitzat					
Revisió de les mesures de seguretat existents en l'accés físic a les instal·lacions. Especialment s'examinen les ubicacions més sensibles com el CPD i l'arxiu.					
Observació					
Comprovació que el CPD disposa de mesures de seguretat adients per garantir la integritat física dels sistemes: climatització, detecció i extinció d'incendis, SAI. **Comprovació que l'arxiu disposa de mesures de seguretat adients per garantir la integritat física del contingut: climatització, detecció i extinció d'incendis.**					
Evidències					
Es comprova l'existència de les mesures de seguretat. **Documentació aportada per la secció de manteniment dels edificis.**					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	11.La seguretat física i ambiental
Control ISO/IEC 27002:2013: 11.2 Equip	
Evitar la pèrdua, dany, robatori o que els actius quedin compromesos juntament amb la interrupció de les operacions de l'organització.	
Treball realitzat	
Revisió de la seguretat física dels llocs del treball.	
Observació	
Es comproven un subconjunt d'espais dels diferents campus. S'exclouen aquells espais o laboratoris destinats a recerca per no estar subjectes a l'abast de l'auditoria.	
Evidències	
Es comprova l'existència de les mesures de seguretat (subministrament, cablejat) **Documentació aportada per la secció de manteniment dels edificis.** **Existència imatge desatesa.** **Inexistència procediment reutilització, de seguretat dels equips fora de les instal·lacions i de política de pantalla transparent.**	
Recomanació	
Crear procediments per reutilitzar els equips, eliminant de forma segura les dades. **Crear procediments per garantir la seguretat dels equips fora de les instal·lacions.**	

Estat:	En curs	**Responsable:**	Informàtica	**Termini:**	1 any
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	12.Operacions de Seguretat
Control ISO/IEC 27002:2013: 12.1 Procediments i responsabilitats operacionals	
Garantir la correcció i seguretat de les operacions a les instal·lacions de processament d'informació.	
Treball realitzat	

Es realitza un qüestionari al responsable de seguretat identificant els responsables de cada servei.
Observació
Es comprova la política els rols definida i les responsabilitats associades.
Evidències
Document de política de seguretat, rols i responsabilitats
Recomanació
No aplica

Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**12.Operacions de Seguretat**
Control ISO/IEC 27002:2013: 12.2 Protecció contra el codi maliciós/malware	
Garantir la protecció contra el malware a les instal·lacions de processament d'informació.	
Treball realitzat	
Es realitza un qüestionari al responsable dels antivirus sobre la seva política d'ús i desplegament.	
Observació	
Es comprova a la gestió centralitzada de l'antivirus el seu desplegament així com l'eina de sandbox per aquells casos sospitosos.	
Evidències	
Informació extreta de la consola centralitzada.	
Recomanació	
No aplica	

Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	12.Operacions de Seguretat				
Control ISO/IEC 27002:2013: 12.3 Còpia de seguretat					
Capitat de recuperació de les dades.					
Treball realitzat					
Es realitza un qüestionari amb el responsable dels sistemes backup. **Es revisa el procediment de backup.** **S'examinen aleatòriament mostres de backup per comprovar la seva validesa.**					
Observació					
Es verifica que les còpies de seguretat realitzades són correctes. **Es verifica el procediment de restauració de còpia de seguretat.**					
Evidències					
Procediment de backup. **Comprovació de les còpies de seguretat analitzades.**					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	12.Operacions de Seguretat
Control ISO/IEC 27002:2013: 12.4 Registre i supervisió	
Registre d'esdeveniments. Generació d'evidència.	

Treball realitzat					
Es realitza un qüestionari amb els administradors de sistemes. **Revisió dels procediments de detecció d'alertes i de logging.**					
Observació					
S'observen les alertes generades i la gestió del sistema de logging.					
Evidències					
Alertes generades per firewalls/IPS **Alertes generades per sistemes de logging**					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	12.Operacions de Seguretat
Control ISO/IEC 27002:2013: 12.5 de control de programari operacional	
Garantir la integritat del sistema.	
Treball realitzat	
Es realitza un qüestionari amb els administradors i desenvolupadors.	
Observació	
S'observa la gestió centralitzada i desplegament de software client. **S'observa en la documentació de projecte l'existència del control de versions de software i les proteccions aplicades.**	
Evidències	
Procediment de gestió de vulnerabilitats. **Requisits projecte implantació del software.**	

Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**12.Operacions de Seguretat**				
Control ISO/IEC 27002:2013: 12.6 La gestió tècnica de la vulnerabilitat					
Prevenir l'explotació de vulnerabilitats tècniques.					
Treball realitzat					
Es realitza un qüestionari al responsable de riscos i el responsable de seguretat. **Es revisen els procediments de detecció de vulnerabilitats.**					
Observació					
S'observa al registre d'incidències la detecció i mitigació de la vulnerabilitat trobada. **Es revisen les eines utilitzades per aquest propòsit.**					
Evidències					
Procediment de gestió de vulnerabilitats.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**12.Operacions de Seguretat**

Control ISO/IEC 27002:2013: 12.7 Sistemes d'informació consideracions d'auditoria					
Minimització de l'impacte de les activitats d'auditoria en els sistemes operatius.					
Treball realitzat					
Es realitza un qüestionari al responsable de seguretat i al responsable de sistemes.					
Observació					
No es disposen de procediments específics per la minimització de l'impacte d'una auditoria sobre els sistemes operatius. **No es disposa d'aplicacions específiques per aquest propòsit a excepció dels sistemes de fitxers en cabina de disc.**					
Evidències					
Informes proporcionats per el software que audita els sistemes de fitxers.					
Recomanació					
Implementar eines de suport que permetin l'obtenció d'informació d'auditoria dels sistemes d'informació minimitzant el seu impacte.					
Estat:	**En curs**	**Responsable:**	**Responsable de Seguretat / Informàtica**	**Termini:**	**6 mesos**
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	13. Seguretat de les comunicacions
Control ISO/IEC 27002:2013: 13.1 Gestió de seguretat de xarxa	
Protegir la xarxa i les seves instal·lacions de suport.	
Treball realitzat	
Es realitza un qüestionari amb el responsable de comunicacions i / o sistemes.	
Observació	
Es comprova l'existència de sistemes tallafocs, IPS/IDS, inspecció de paquets a través de l'antivirus, WAF i control d'aplicacions.	

Es realitza un anàlisi de la seva configuració.					
Evidències					
Configuració dels mecanismes de protecció. **Informes del sistema de tallafocs+IPS+antivirus.**					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**13. Seguretat de les comunicacions**				
Control ISO/IEC 27002:2013: 13.2 La transferència d'informació					
Garantir la seguretat d'aquella informació transferida de l'organització amb qualsevol altri.					
Treball realitzat					
Es comprova els procediments de cessió d'informació.					
Observació					
Es verifica l'existència d'un procediment de cessió i transferència d'informació					
Evidències					
Procediment de cessió d'informació.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	14.Sistema d'adquisició, desenvolupament i manteniment				
Control ISO/IEC 27002:2013: 14.1 Requisits de seguretat dels sistemes d'informació					
Assegurar que la seguretat informàtica és una part integral dels sistemes d'informació a través de tot el cicle de vida incloent els serveis oferts a través de xarxes públiques.					
Treball realitzat					
Es realitza un qüestionari al responsable de seguretat i al responsable de les aplicacions, i si escau el responsable de sistemes.					
Observació					
S'observa que els serveis i aplicacions estan protegits a través del tallafocs (WAF+IPS). **Aquesta protecció es realitza de forma centralitzada.**					
Evidències					
Documentació dels projectes i serveis, especificacions de seguretat incloses en ells.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	14.Sistema d'adquisició, desenvolupament i manteniment
Control ISO/IEC 27002:2013: 14.2 Seguretat en els processos de desenvolupament i suport	
Aplicació de criteris de disseny segur dins el cicle de vida de desenvolupament de sistemes d'informació.	
Treball realitzat	
Es realitza un qüestionari amb el responsable de projectes i aplicacions.	
Observació	
Es comprova dins l'especificació dels projectes les característiques de seguretat necessàries.	

Evidències					
Contractes amb proveïdors de serveis. **S'observa que els serveis i aplicacions estan protegits a través del tallafocs (WAF+IPS).**					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**14.Sistema d'adquisició, desenvolupament i manteniment**				
Control ISO/IEC 27002:2013: 14.3 Dades de prova					
Les dades de prova han de ser degudament generades i controlades.					
Treball realitzat					
Realització d'un anàlisi de dades en alguns entorns de preproducció i desenvolupament.					
Observació					
S'observa l'ús de dades reals en alguns entorns sense protecció adient.					
Evidències					
Consultes realitzades a les bases de dades.					
Recomanació					
Implementar un protocol per dissasociar les dades en entorns de preproducció , o bé, implementar els mateixos mecanismes de seguretat.					
Estat:	**En curs**	**Responsable:**	**Informàtica**	**Termini:**	**6 mesos**
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	15.Les relacions amb proveïdors
Control ISO/IEC 27002:2013: 15.1 Seguretat de la informació en relació amb els proveïdors	
Existència de polítiques i procediments per protegir la informació de l'organització que és accessible a empreses externes.	
Treball realitzat	
Revisió dels serveis externalitzats. Es revisa els nivells de permisos i accessos del personal extern que treballa a l'organització.	
Observació	
Es comprova que el personal extern aplica les mesures de seguretat de l'organització. **Es comprova que en els acords de prestació de serveis les empreses no estan obligades a aplicar el mateix nivell de seguretat.**	
Evidències	
Acords de confidencialitat. **Documentació de prestació de serveis.**	
Recomanació	
Introduir en els acords de prestació de serveis l'obligatorietat de compliment de les condicions de seguretat de l'organització.	

Estat:	**En curs**	**Responsable:**	**Informàtica**	**Termini:**	**6 mesos**
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	15.Les relacions amb proveïdors
Control ISO/IEC 27002:2013: 15.2 La gestió de la prestació de serveis de proveïdors	
El servei proporcionat per proveïdors externs ha de ser revisat i auditat segons els contractes i acords establerts.	
Treball realitzat	

Es revisen els aspectes contractuals en la contractació de tercers (acords de confidencialitat, acords de nivell de servei).
Observació
Es comprova que el personal extern aplica les mesures de seguretat de l'organització.
Evidències
Acords de confidencialitat. **Documentació de prestació de serveis.**
Recomanació
Introduir en els acords de prestació de serveis l'obligatorietat de compliment de les condicions de seguretat de l'organització.

Estat:	**En curs**	**Responsable:**	**Informàtica**	**Termini:**	**6 mesos**
CONCLUSIÓ:			**NO CONFORME**		

ÀREA	**16.Gestió d'incidents de seguretat d'informació**
Control ISO/IEC 27002:2013: 16.1 Gestió d'incidents de seguretat de la informació	
Existència de gestió de procediments, responsabilitats, recol·lecció d'evidències i incidents.	
Treball realitzat	
Revisió del procediment de gestió d'incidents	
Observació	
Es revisen els documents que recullen el registre d'incidències així com els procediments relacionats.	
Evidències	
Registre d'incidències. **Procediment de registre d'incidències.**	
Recomanació	
No aplica	

Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci**
Control ISO/IEC 27002:2013: 17.1 Continuïtat seguretat de la informació	
La continuïtat de la seguretat d'informació ha de ser planejada, implementada i revisada com a part integral dels sistemes de continuïtat de negoci de l'organització.	
Treball realitzat	
Revisió dels plans de continuïtat de negoci.	
Observació	
Comprovació que els plans de continuïtat són revisats i provats periòdicament. **Els procediments estan actualitzats i vigents.**	
Evidències	
Documentació del procediment del pla de proves.	
Recomanació	
No aplica	

Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci**
Control ISO/IEC 27002:2013: 17.2 Les redundàncies	

Assegurar la disponibilitat dels serveis de processament d'informació.
Treball realitzat
Revisió de la documentació dels sistemes instal·lats. **Revisió del registre d'incidències.** **Documentació de prestació de serveis.**
Observació
Es comprova l'existència d'un pla de proves anual i manteniment del mateix.
Evidències
Documentació del procediment del pla de proves.
Recomanació
No aplica

Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**18.Compliment**
Control ISO/IEC 27002:2013: 18.1 Compliment dels requisits legals i contractuals	
Assegurar el compliment de les obligacions legals, reglamentàries o contractuals relacionades amb la seguretat de la informació.	
Treball realitzat	
Revisió de la realització d'auditories internes. Revisió de polítiques .	
Observació	
Existeix una planificació d'auditoria interna bianual per tal d'assegurar que es compleixen amb les polítiques establertes.	
Evidències	
Documentació de prestació de serveis.	

Documentació de contractes realitzats.					
Recomanació					
No aplica					
Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

ÀREA	**18.Compliment**
Control ISO/IEC 27002:2013: 18.2 Revisions de la seguretat de la informació	
Garantir que la seguretat informàtica és implementat i operat d'acord amb les polítiques i procediments de l'organització.	
Treball realitzat	
Revisió de la realització d'auditories internes. Revisió de polítiques .	
Observació	
Existeix una planificació d'auditoria interna bianual per tal d'assegurar que es compleixen amb les polítiques establertes.	
Evidències	
Documentació dels sistemes afectats per la LOPD. **Documentació genera a partir del Comitè de Seguretat.** **Documentació generada a partir de l'auditoria interna.**	
Recomanació	
No aplica	

Estat:	No aplica	**Responsable:**	No aplica	**Termini:**	No aplica
CONCLUSIÓ:			**CONFORME**		

8. Resultats de l'auditoria

L'auditoria ha consistit en la realització de diferents activitats:

- Entrevistes amb els responsables de cada àrea
- Visites a les instal·lacions
- Revisió de la documentació aportada
- Proves insitu sobre el funcionament dels sistemes.

Aquestes activitats han srvit per mesurar el grau de maduresa dels diferents dominis i objectius de control de la Norma ISO/IEC 27002: 2013.

El grau de maduresa en què es troben els diferents dominis ha millorat globalment tal com mostre la següent taula:

ÀREA	CMM (Anterior)	CMM (Futura)
5. Polítiques de la Seguretat de la Informació	0%	90%
6.Organització de la seguretat de la informació	31%	50%
7. La seguretat dels recursos humans	7%	50%
8. Gestió d'actius	23%	95%
9. Control d'accés	30%	50%
10.Criptografia	0%	50%
11.La seguretat física i ambiental	45%	50%
12.Operacions de Seguretat	35%	90%
13.Seguretat de les comunicacions	44%	95%
14.Sistema d'adquisició, desenvolupament i manteniment	37%	50%
15.Les relacions amb proveïdors	12%	50%
16.Gestió d'incidents de seguretat d'informació	10%	95%
17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	9%	90%
18.Compliment	28%	95%

Els resultats de l'anàlisi de cada un dels controls de la ISO27002 mostren un total de **8** "No Conformitats" que hauran de ser corregides:

- 6.2 Els dispositius mòbils i el teletreball
- 7.1 Amb anterioritat a l'ocupació
- 7.3 Terminació i canvi d'ocupació
- 9.1 Els requisits de negoci de control d'accés
- 11.2 Equip
- 12.7 Sistemes d'informació consideracions d'auditoria
- 14.3 Dades de prova
- 15.1 Seguretat de la informació en relació amb els proveïdors
- 15.2 La gestió de la prestació de serveis de proveïdors

Detall:

NUMERAL DE LA NORMA	DESCRIPCIÓ NORMA	DESCRIPCIÓ	TIPOLOGIA
6.2.1	Polítiques per dispositius mòbils	No està definida cap política ni normativa al respecte. No es realitza cap tipus de control.	NO CONFORME
6.2.2	Teletreball	No està definida cap política ni normativa al respecte. No es realitza cap tipus de control.	NO CONFORME
6.2.2	Teletreball	Revisió i millora del servei VPN	MILLORA
7.1.2	Termes i condicions d'ocupació	Existència de procediments de contractació sense acords de confidencialitat en alguns departaments.	NO CONFORMITAT MENOR
7.3.1	Finalització o canvi de les responsabilitats d'ocupació	No es revisa els materials en possessió de l'empleat quan aquest finalitza la prestació de serveis.	NO CONFORME
9.1.1	Política de control d'accés	No es realitzen controls d'accés físic suficient.	NO CONFORMITAT MENOR
11.2.5	Retirada dels actius	No existeix procediment	NO

			CONFORMITAT
11.2.6	Seguretat dels equips i actius fora de les instal·lacions	No existeix procediment ni mesures de seguretat addicionals.	NO CONFORMITAT
11.2.7	L'eliminació segura o la reutilització dels equips	No existeix procediment establert.	NO CONFORMITAT MENOR
11.2.9	Netejar l'escriptori i la política de pantalla transparent	No s'aplica actualment de forma homogènia.	MILLORA
12.7.1	Sistemes d'informació controls d'auditoria	No es disposen de les eines adequades per realitzar auditories.	NO CONFORMITAT MENOR
14.3.1	Protecció de dades de prova	S'identifiquen dades reals en entorns de preproducció.	NO CONFORMITAT MENOR
15.1.1	Política de seguretat de la informació de relacions amb els proveïdors	No s'inclouen clausules específiques de seguretat en els acords de prestació de serveis.	NO CONFORMITAT
15.1.2	Abordar la seguretat dins dels acords amb proveïdors	No s'inclouen clausules específiques de seguretat en els acords de prestació de serveis.	NO CONFORMITAT MENOR
15.2.1	Seguiment i revisió dels serveis de proveïdors	No es realitza seguiment.	MILLORA