PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ DE LA UNIF

Nom Estudiant: ALBERT PINTU PLA

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

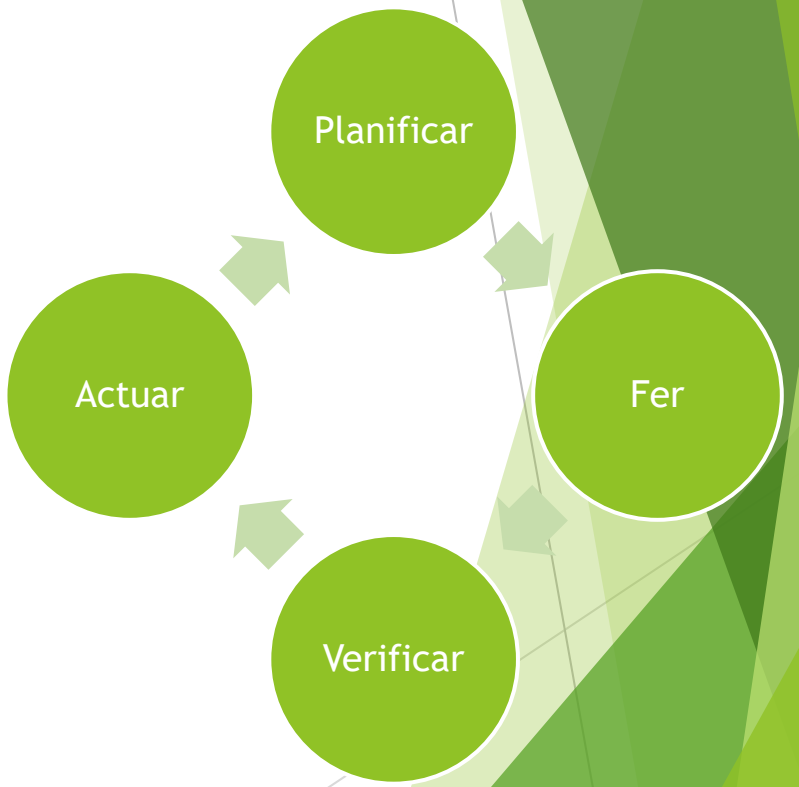
Consultor: ARSENIO TORTAJADA GALLEGO

Data Lliurament: 4/1/2017

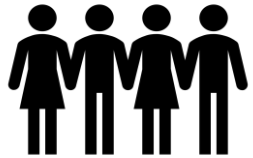
Índex

Descripció del projecte I

- El projecte presentat com a Treball Fi de Màster té com a objectiu general analitzar i estudiar l'estat dels sistemes de seguretat d'una organització per poder desenvolupar un Sistema de Gestió de la Seguretat a la mateixa organització.
- En aquest treball ens basarem sobre una organització real, una Universitat, però a efectes de confidencialitat durant tot el TFM l'organització serà anomenada com a "UNIF – Universitat Fictícia". Així mateix alguns aspectes tècnics i dades proporcionades poden ser omeses o canviades amb dades fictícies a afectes de mantenir aquesta confidencialitat.
- La metodologia empleada en el procés de millora continua es basarà en el cicle de Deming (Planificar, Fer, Verificar i Actuar) .



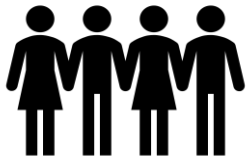
Descripció del projecte II: La UNIF, xifres



12000 alumnes

Campus A

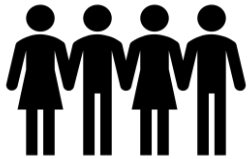
CPD A



2000 professors

Campus B

CPD B



1000 personal

Campus C

CPD C

Descripció del projecte III: La UNIF, serveis TIC

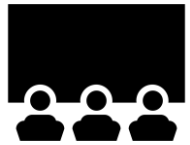
- Serveis TIC oferts
  - Aula virtual (moodle)
  - Suport a aules de dòcencia
  - Suport a biblioteca
  - Gestió dels centres de càlcul
  - Supercomputació
  - Gestió i manteniment de la xarxa
  - Manteniment de la infraestructura de sistemes
  - Administració electrònica
  - Suport als usuaris
  - Normatives TIC i LOPD
- Infraestructures (tecnologies)
  - Serveis de directori (Novell/Windows)
  - Servidors d'aplicacions (Tomcat/Weblogic)
  - Bases de dades (Mysql, Oracle, MSSQL Server)
  - Cabines de disc (EMC, NetApp)
  - Proxies
  - Cablejat estructurat i fibra òptica
  - Connexions a l'anella cientifica
  - Sistemes operatius clients
  - Dispositius mòbils

Descripció del projecte IV: Objectius del pla director

- 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.

Descripció del projecte V: Abast

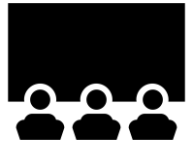
- L'abast d'aquest projecte ha consistit en la realització d'un Pla de director de Seguretat, que inclou tota la infraestructura de l'àrea IT dels serveis centrals. Entendrem com a serveis centrals aquells serveis i processos que donen servei de forma homogènia a tota la comunitat, per exemple, serveis d'autenticació, aplicacions corporatives, etc.
- Aquest treball no ha inclòs 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.



Serveis centrals

Unitats acadèmiques

Facultats



Centres de recerca

Fases del projecte

El projecte s'ha realitzat segons les següents fases:

- FASE I : Situació actual, contextualització, objectius i anàlisi diferencial.
- FASE II : Sistema de Gestió Documental.
- FASE III : Anàlisi de riscos.
- FASE IV : Propostes de projectes.
- FASE V : Auditoria de compliment ISO/IEC 27002.
- FASE VI : Presentació de resultats, i resum executiu que acompanya la memòria del projecte.

Fase I: Situació Actual

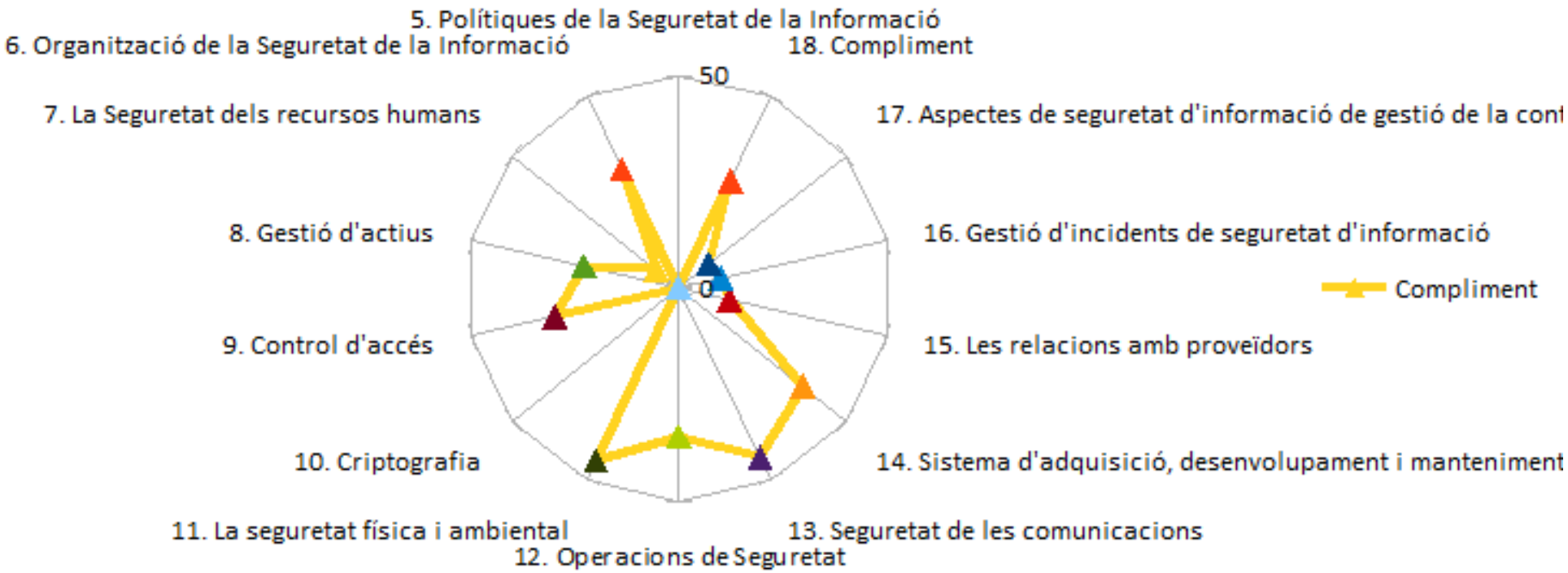
Un cop analitzada l'organització durant la Fase I obtenim:

- La situació actual de la UNIF
- La contextualització del negoci i l'abast del projecte
- Els objectius del projecte i del pla director de seguretat
- L'anàlisi diferencial de la ISO

Específicament els resultats de la Fase I són:

- L'abast del projecte, concentrat als serveis centrals
- La falta de seguretat en molts aspectes (formació, equipament, procediments, etc)
- Absència de documentació degudament actualitzada
- Falta de competències específiques en matèria de seguretat
- Falta assegurar molts aspectes respecte a les dimensions de seguretat (autenticitat, confidencialitat, integritat, disponibilitat i traçabilitat)

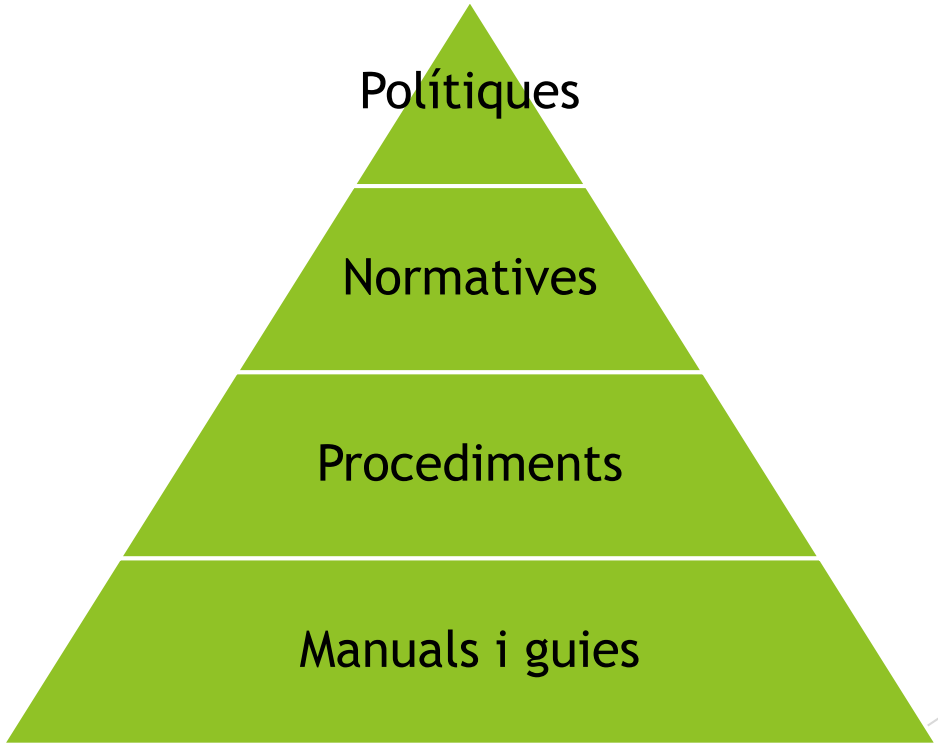
Fase I: Anàlisi diferencial



Fase II : Sistema de Gestió Documental

Durant aquesta fase es creen els següents documents:

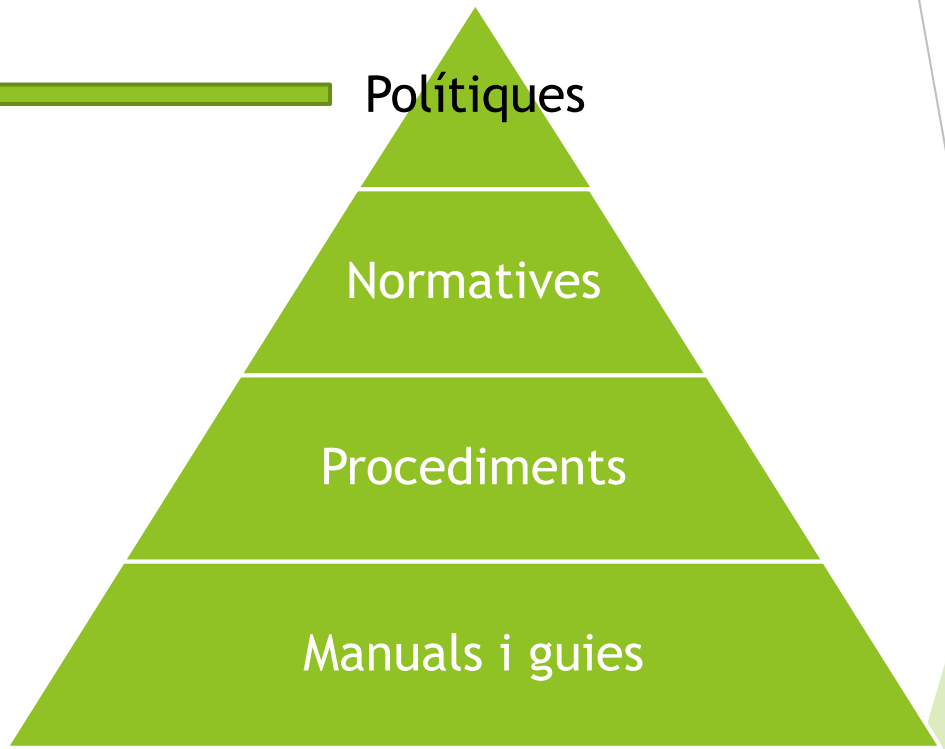
- Política de Seguretat
- Procediment d'auditories internes
- Gestió d'indicadors
- Procediment de revisió per direcció
- Gestió de rols i responsabilitats
- Metodologia d'anàlisi de riscos
- Declaració d'aplicabilitat



Fase II : Sistema de Gestió Documental

POLÍTICA DE SEGURETAT

- Ús dels sistemes informàtics.
- Identificació i control d'accés al sistema.
- La confidencialitat de la informació.
- Ús dels serveis.
- Incidències i infraccions de seguretat de la informació.



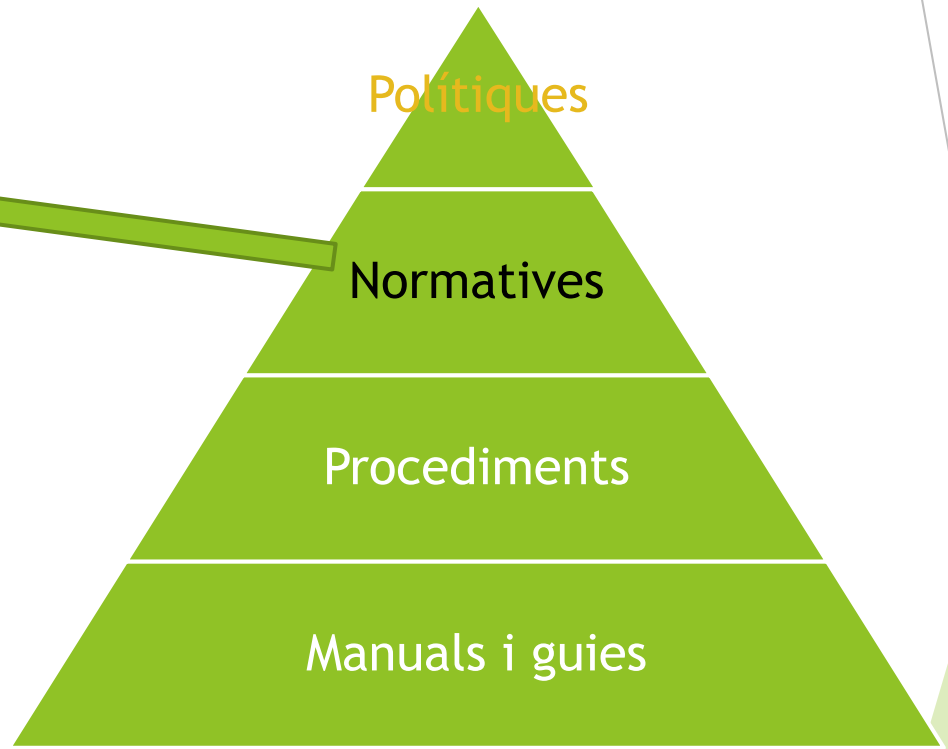
Fase II : Sistema de Gestió Documental

GESTIÓ DE ROLS I RESPONSABILITATS

GESTIÓ D'INDICADORS

DECLARACIÓ D'APLICABILITAT

- Estructura Organitzativa sobre la seguretat
- Determinar l'eficàcia de les mesures de seguretat implementades
- Controls a implementar en el SGSI



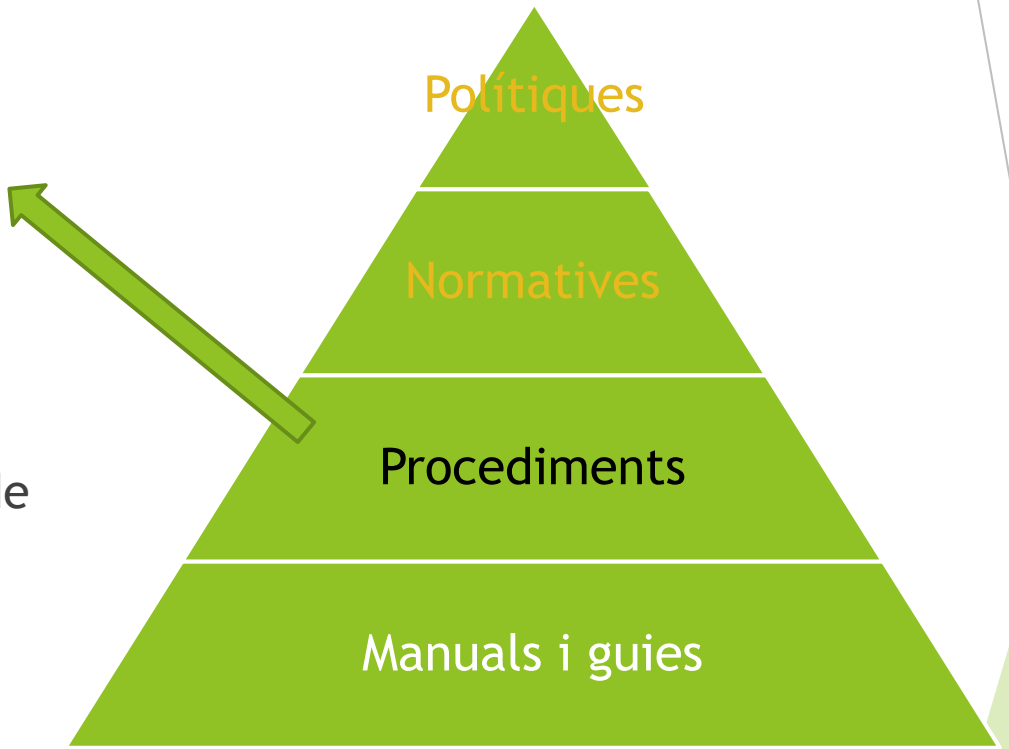
Fase II : Sistema de Gestió Documental

PROCEDIMENT D'AUDITORIES INTERNES

PROCEDIMENT DE REVISIÓ PER DIRECCIÓ

METODOLOGIA DE ANÀLISIS DE RISCOS

- Estructura Organitzativa sobre la seguretat
- Determinar l'eficàcia de les mesures de seguretat implementades
- Controls a implementar en el SGSI



Fase II : Sistema de Gestió Documental

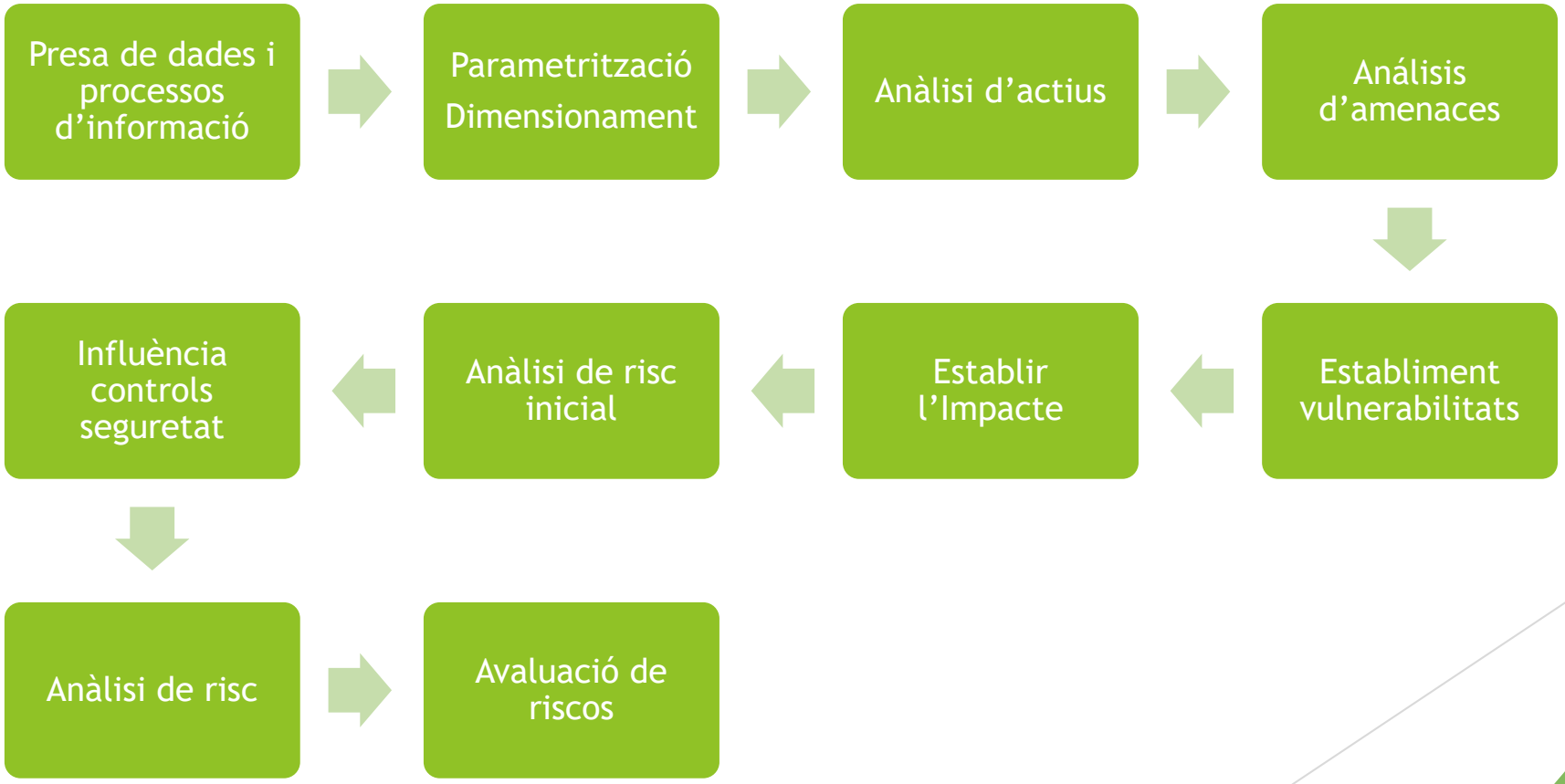
- RESULTATS
  - S'ha creat els documents principals dels que ha de disposar la organització
  - S'ha revistat la documentació per tal que sigui comprensible per a tots els usuaris augmentant el compliment de la mateixa
  - S'ha identificat al document d'aplicabilitat quins elements de la normativa ISO són aplicables a la nostra organització
  - S'ha posat la primera pedra perquè aquestes documentacions es revisin periòdicament actualitzant i posant al dia el seu contingut quan sigui necessari

Fase III : Anàlisi de Riscos

- A la Fase III s'ha realitzat l'anàlisi de riscos de l'organització, on s'inclouen:
  - L'inventari d'actius
  - La valoració d'actius, seguint la metodologia MAGERIT
  - Valoració de la criticitat seguint les dimensions de seguretat (ACIDT)
  - L'anàlisi d'amenaces
  - L'impacte potencial de les amenaces
  - El nivell de risc acceptable i residual

Fase III : Anàlisi de Riscos

La metodologia utilitzada és MAGERIT v.3



Fase III : Anàlisi de Riscos

Inventari d'actius

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.

Valoració d'actius

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

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

Fase III : Anàlisi de Riscos

Valoració per dimensions de seguretat

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

Taula de valoracions

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

Fase III : Anàlisi de Riscos

Anàlisi d'amenaces

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	

Actius i dimensions de seguretat

ACTIU	FREQ	ASPECTES CRÍTICS				
		A	C	I	D	A
Centre de Càlcul 1 (CPD)	Baixa		100	50	100	
Centre de Càlcul 2 (CPD)	Baixa		100	50	100	
Centre de Càlcul 3 (CPD)	Baixa		100	50	100	
Arxiu.	Baixa		100	50	100	
RITI 1. (Recinte d'instal·lacions de Telecomunicacions)	Baixa		100	50	100	
RITI 2.	Baixa		100	50	100	
RITI 3.	Baixa		100	50	100	
AMENACES						
Incendi	Remota				100	
Inundació	Remota				50	
Desastre natural	Remota				100	
Foc i danys per aigua	Baixa				50	
Degradació de suports i equipament	Baixa				50	
Avaria climatització (temperatura i humitat)	Baixa				50	
Fallada subministrament elèctric	Baixa				50	
Avaria física	Baixa				50	
Interrupció d'altres serveis i subministres essencials	Baixa				50	
Errors humans (usuaris)	Baixa				50	

Fase III : Anàlisi de Riscos

Impacte potencial

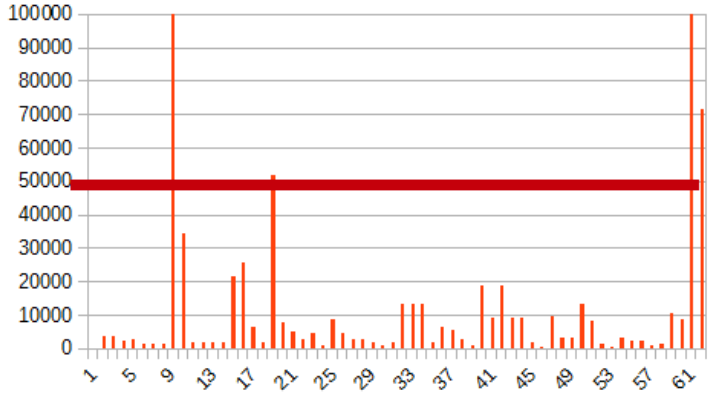
CODI	ASPECTES CRÍTICS					%IMPACTE					IMPACTE POTENCIAL				
	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
I.1	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.2	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.3	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.4	8	6	9	9	8		100	50	100		0	6	4,5	9	0
I.5	7	6	9	9	8		100	50	100		0	6	4,5	9	0
I.6	7	6	8	9	8		100	50	100		0	6	4	9	0
I.7	7	6	8	9	8		100	50	100		0	6	4	9	0

Risc Intrínsec = Impacte Potencial x Freqüència

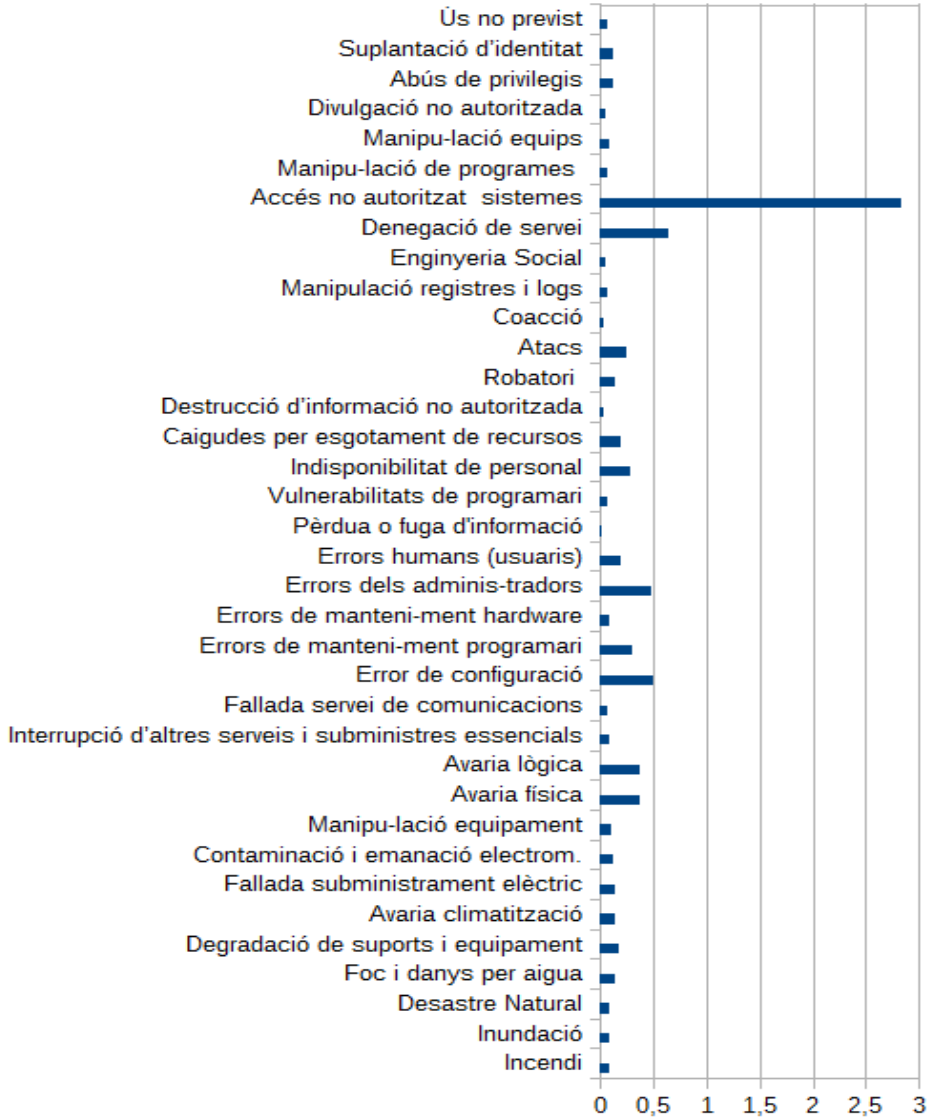
CODI	FREQ	VALOR FREQ	ASPECTES CRÍTICS					RISC				
			A	C	I	D	A	A	C	I	D	A
I.1	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.2	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.3	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.4	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.5	Baixa	0,005	0	6	4,5	9	0	0	3	2,25	4,5	0
I.6	Baixa	0,005	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

Fase III : Anàlisi de Riscos Resultats

Llindar > 50000



Amenaces



Fase III : Anàlisi de Riscos Resultats

- 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.

Fase IV : Propostes de projectes

Projectes de millora

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.

Fase IV : Propostes de projectes

Projectes

- 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.
- Publicació i resolució efectiva de les polítiques de seguretat
  - **Objectiu**: Definir, revisar, aprovar i posar en producció la política general de seguretat de la informació, aquelles polítiques que se'n puguin derivar, la definició de les metodologies, indicadors i en general tota la documentació relativa al SGSI.
- Pla de conscienciació i capacitació del personal
  - **Objectiu**: Generar consciència entre el personal intern de l'organització, personal extern i proveïdors respecte a la posició de la UNIF sobre la seguretat de la informació. Especialment és rellevant per aquest objectiu capacitar i donar els coneixements necessaris al personal intern responsable de gestionar diferents aspectes de la seguretat de la informació. Aquesta capacitació inclou des del coneixement de la pròpia ISO 27001:2013 a la gestió de vulnerabilitats i incidents.

Fase IV : Propostes de projectes

Projectes

- 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.
- 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.
- Implementar sistemes d'auditories i anàlisi continu 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.

Fase IV : Propostes de projectes

Projectes

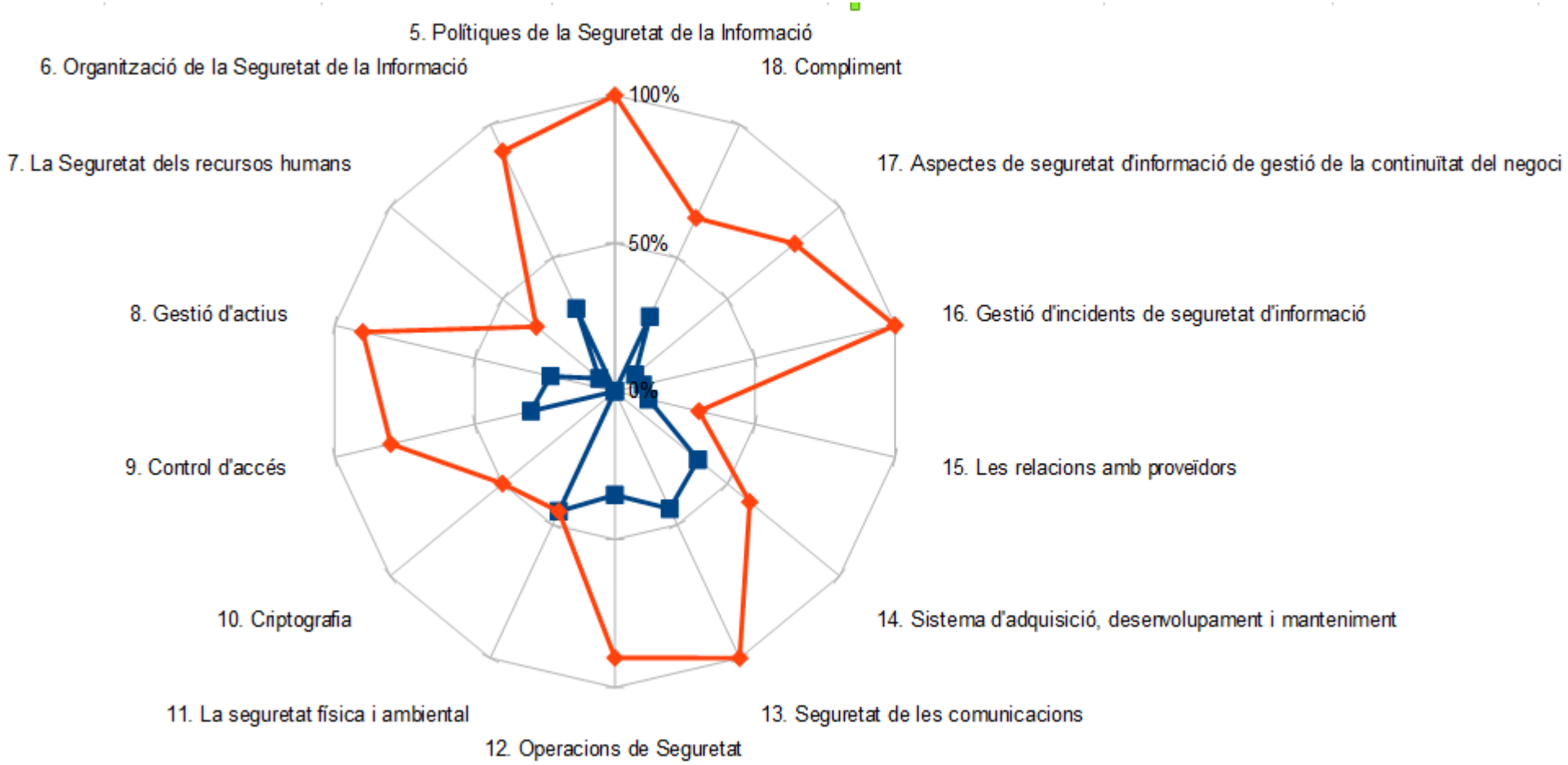
- Implementar tallafocs de nova generació
  - **Objectiu**: Adquirir i implementar nous tallafocs perimetrals i interns de nova generació (capa 7). Permetran redefinir i ajustar les necessitats de connectivitat amb els avantatges de les eines incorporades de IPS i antivirus que permeten escanejar el trànsit en temps real juntament amb les eines d'auditoria de xarxa.
- Auditoria i control de xarxa centralitzada
  - **Objectiu**: Avaluar, adquirir i implementar solucions que permetin tenir un quadre de control global de la infraestructura de xarxa. Així mateix aquesta solució integrarà aspectes de configuració d'infraestructura que permetrà assegurar la correcta configuració de cada element de xarxa. També proporcionarà una monitorització d'ús i rendiment.
- Gestió centralitzada política d'antivirus
  - **Objectiu**: Avaluar i adquirir una solució que permeti centralitzar la gestió dels clients antivirus, a ser possible de més d'un proveïdor. Això permetrà donar un millor suport al projectes de gestió de vulnerabilitats i gestió d'incidents de seguretat. Aquesta solució hauria de permetre la millora de participació dels serveis de helpdesk en la getió d'incidents en els equips clients finals (workstations).

Fase IV : Propostes de projectes

Projectes

- Implementar nous sistemes de backup
  - **Objectiu**: Avaluar les necessitats actuals de backup incloent tots els sistemes disponibles i adquirir productes que permetin satisfer millor les necessitats. S'establirà un període d'avaluació inicial molt llarg per tal que tots els departaments tinguin el temps suficient per determinar de forma específica les seves necessitats. Aquestes necessitats inclouran tant conceptes de capacitat com velocitat de recuperació.
- 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.

Fase IV : Propostes de projectes
Resultats



Fase V : Auditoria de compliment

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**		

Fase V : Auditoria de compliment

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

Fase V : Auditoria de compliment

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

Conclusions, què s'ha fet?

- S'ha observat la situació actual de l'organització
- S'ha identificat les amenaces i els riscos
- S'ha creat documentació necessària per l'organització
- S'ha creat un inventari d'actius
- S'ha proposat projectes de millora
- S'ha avaluat l'organització segons la ISO 27002
- S'ha millorat la seguretat de la organització
- S'ha assentat les bases per un model de millora continua

Conclusions

- La seguretat afecta a tots els actius de l'organització
- La millora constant afecta positivament sobre la seguretat
- Per complir les normatives legals s'ha de tenir especial consideració a la seguretat
- La continuïtat del negoci depèn en bona part de la seguretat
- La seguretat té beneficis sobre l'eficiència dels processos dins de l'organització
- La formació continua dels empleats esdevé prioritària
- És imprescindible el compromís de la direcció

Conclusions, millora continua

- Implementar nous controls
- Mantenir actualitzat l'inventari d'actius i els riscos associats
- Revisar la documentació
- Mantenir la infraestructura sempre actualitzada
- Disposar d'una monitorització proactiva de la xarxa
- Continuar amb els plans de conscienciació

Final de la presentació

- MOLTES GRÀCIES