Universitat Oberta de Catalunya

Màster Interuniversitari en Seguretat de les TIC (MISTIC)

TREBALL DE FINAL DE MÀSTER

Elaboració d'un Pla de Seguretat de la Informació

Jonatan López Romera

Presentació TFM

Organització de la confecció Pla de Seguretat de la Informació (PDS)

1. Presentació del cas d'ús
2. Presentació del Pla Director
3. ESTAT DEL RISC: Identificació i valoració dels Actius i Amenaces
4. Auditoria de compliment de la ISO/IEC 27002:2005
5. Propostes de millora per l'organització
6. Conclusions del PDS

INDEX DE L'APARTAT

PRESENTACIÓ CAS D'US

- Dades rellevants de l'organització
- Dades rellevants dels Sistemes de Informació
- Estat actual de la seguretat dels S.I.
  - Situació Actual
  - Mesures de seguretat Presents
- Motivació per la creació del PDS
  - Abast del PDS

Dades rellevants de l'empresa

- Es realitzarà un PDS complert sobre una **multinacional a nivell europeu** del sector de la gran distribució en el **sector alimentari**, a la seva divisió de refrigerats per la regió Ibérica.

- **"UOC Postres S.A."**

- Les seves àrees on desenvolupa la seva activitat econòmica son:

  - **Fabricació** de productes refrigerats de Marca.
    - Productes de Marca.
    - Productes de "Marca De Distribució(MDD)" (també conegut com "Marca Blanca").

  - **Comercialització** als mercats Espanyol i Portuguès.
    - Comercialització Marca per a grans comptes.
    - Comercialització Marca per capil·laritat (petits clients).
    - Comercialització "Marca Blanca"

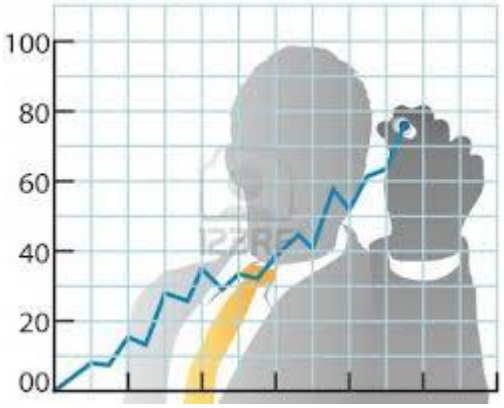
  - **Distribució** del producte.

Dades rellevants de l'empresa

- Dades d'interès de l'organització:
  - 1 Fàbrica a Espanya
    * A nivell Europa existeixen 7 fàbriques per produir el catàleg complert de productes.
  - 2 Headquarters (ES + PT)
  - 7 Oficines comercials (ES + PT)
  - 2 Centres de Distribució (ES + PT)

  - **650 Treballadors a Espanya**
  - **132 Treballadors a Portugal**

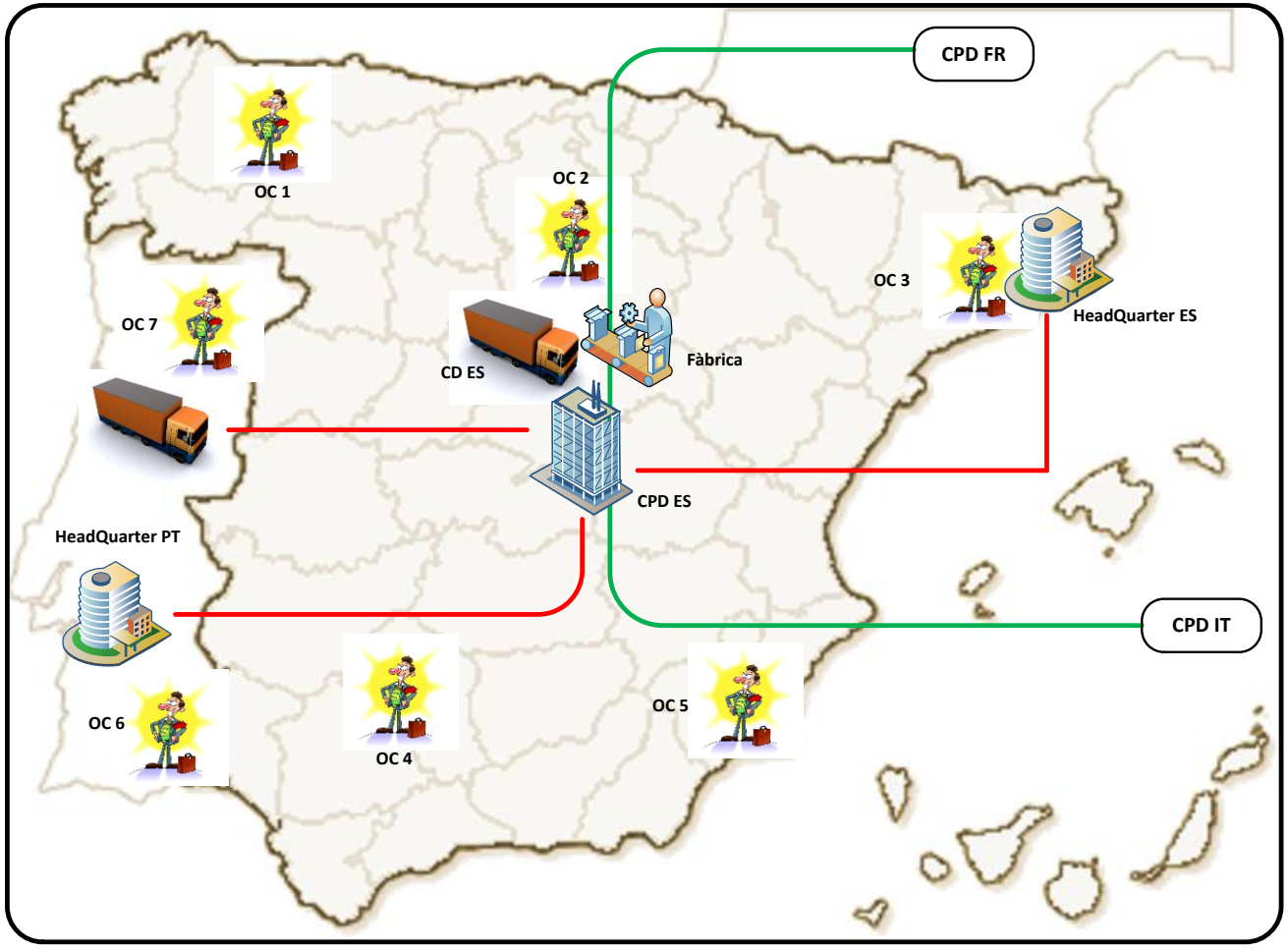
  - **Quota de mercat** (marca pròpia):
    - **ES 3%**
    - **PT 18,7%**



  - **Quota de mercat MDD** (respecte MDD Total):
    - ES 89%
    - PT 52%

  - Centres de Procés de Dades (CPD): 1

Localització Geogràfica de l'organització



Dades rellevants del S.I.

- Sistemes Bàsics / estàndards

  - **Sistema de Correu.**
    (Microsoft Exchange 2003)

  - **Sistema d'Enterprise Resource Planning *(ERP - SAP)***
    - *Donant cobertura als mòduls de* ***comptabilitat, facturació, control de gestió, vendes, Business Intelligence, Facturació logística i RRHH.***
    - ***Servei Distribuït des de el CPD de França.***

  - **Sistemes de comunicació interna.**
    (Microsoft Office Communicator 2007)

  - **Sistema d'intranet corporativa.** Es tracta d'un portal corporatiu utilitzat per tots els usuaris de la companyia per tal de consultar informacions o realitzar processos establerts per ser realitzats per aquest mitjà (ex. Liquidació de despeses, etc.)

  - **Eines bàsiques de la estació de treball.** (SO, antivirus, Office, plugins, etc.)

Dades rellevants del S.I.

- Sistemes concrets de l'organització

  - **Sistema de gestió de magatzems (INFOLOG + SGANL).** S. I. Utilitzats per la gestió complerta de tots els magatzems de l'organització mitjançant la infraestructura hardware de radiofreqüència implementada per representar la lògica del negoci.

  - **Sistema de gestió de manteniments i serveis tècnics (PRISMA).** Gestió del manteniment i reparacions de tota la maquinaria de les fàbriques del grup implementant un estocs comú per les diferents fàbriques de cara a obtenir una optimització de l'immobilitzat que suposa l'inventari. S'encarrega de gestionar l'inventari, el manteniment preventiu i proactiu, i la gestió d'actuacions de l'equip tècnic.

  - **Sistema de planificació de la producció (FUTURMASTER).** Sistema de planificació en funció de les previsions de vendes a mig (2/4 setmanes) i llarg termini (5 a 12 setmanes vista) per tal d'evitar les situacions de ruptura per falta de materials o sobre produccions. Es troba interconnectada a les diferents fonts de informació que permeten realitzar les previsions.

    - **Servei Distribuït des de el CPD de França**

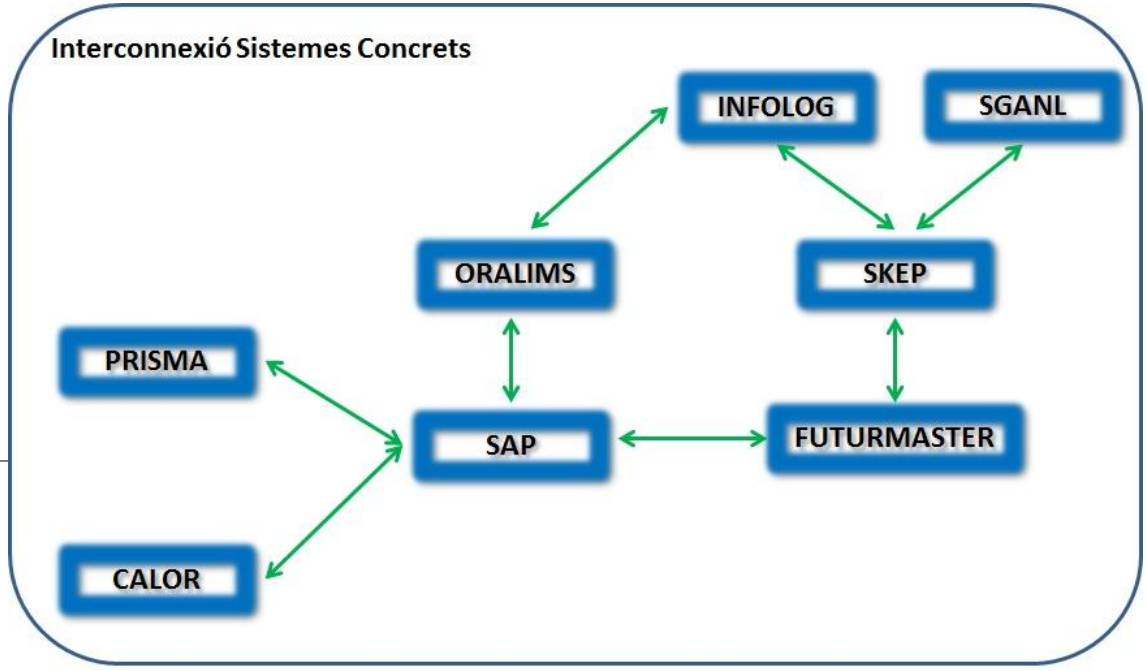
Dades rellevants del S.I.

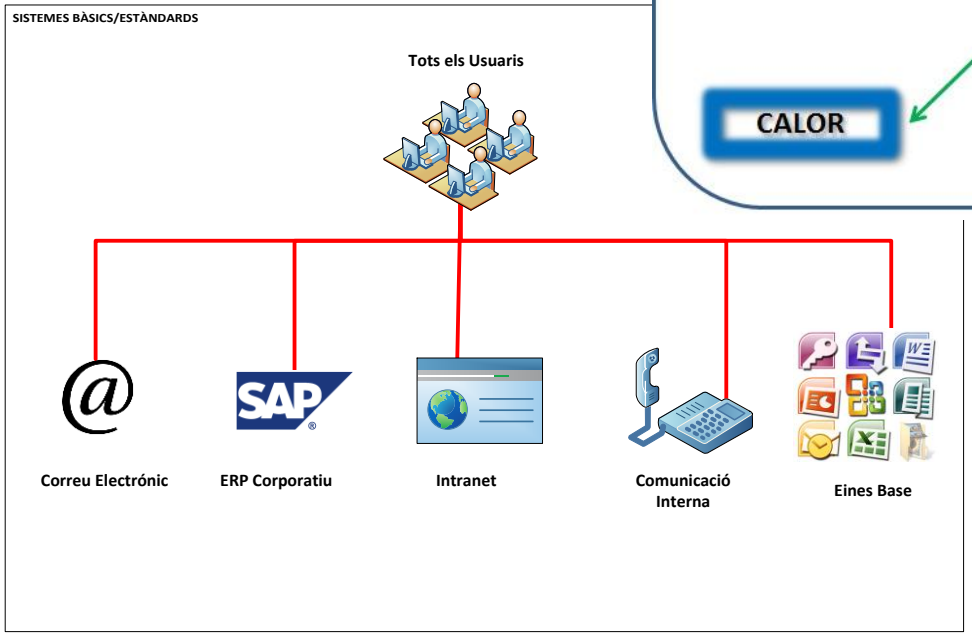
- **Sistema de planificació de Necessitats (SKEP).** En aquest cas es tracta de la planificació a curt termini (setmana actual) de cara a optimitzar els cicles de producció industrial en funció a la materialització de les comandes dels clients i la disponibilitat dels materials.

- **Sistema de gestió de la qualitat (ORALIMS).** S'utilitza al departament de qualitat per gestionar la qualitat del producte durant tota la fase de producció i distribució per garantir la traçabilitat complerta del producte.

- **Sistema gestió punt de Venda (CALOR).** S'encarrega de gestionar totes les comandes que no provenen pel canal de gran distribució a través de sistemes automatitzats de recepció de fitxers per e-mail, gestió telefònica, gestió agrupada per majorista i presa manual mitjançant terminals mòbils des de l'equip de força de ventes.

Esquema Global dels S.I. utilitzats





*** Dintre de la memòria d'aquest TFM trobem tota la descripció tècnica i detallada de tots els sistemes.*

Estat actual Seguretat dels S.I.

- Situació Actual:
  - **Mai** s'ha realitzat un pla de seguretat de la informació.
  - Les mesures existents han estat preses sense l'estudi complert de la seva necessitat i justificació.

    CONSECUENCIA:
    - **Mesures inexistents**
    - **Mesures sobredimensionades**
    - **Desconeixement de les amenaces**
    - **Desconeixement dels Riscos e Impacte**
  - No existeix ***"tractament intern" per la seguretat de la informació.***
    - **Cap normativa de seguretat**
    - **Inexistència de pla de contingències**
    - **Inexistència d'un anàlisi de riscos**

- VALORACIÓ DE LA SITUACIÓ:
  - **Nivell Baix de seguretat de la informació**

Estat actual Seguretat dels S.I.

- Mesures de Seguretat Presents:

- **Seguretat física sobre el CPD:**
  - Protecció contra incendis.
  - Accés restringit i controlat pel personal autoritzat.
    - Control exhaustiu personal i material extern.
- **A nivell de les comunicacions:**
  - Acords de servei e integritat amb el proveïdors.
  - Xarxa propietària per l'organització.
  - Accés / Sortida de xarxa monitoritzat i controlat.
  - Infraestructura de xarxa i línies redundants per garantir el servei.
- **Infraestructura dels magatzems:**
  - Donat el servei constant i valuós dintre de l'organització que representen el magatzems i la gestió del mateixos, tota la seva infraestructura es troba de forma "redundant" per tal de poder garantir el servei 24 hores x 7 dies que es treballa en aquestes instal·lacions.

Estat actual Seguretat dels S.I.

- **A nivell de sistemes:**
  - Procediment de instal·lació inicial per cada sistema.
  - Procediment de recuperació per cada sistema.
  - Procediment de gestió de les copies de seguretat.
  - No son desenvolupaments interns:
    - Existeix contracte de manteniment amb el desenvolupador.
  - Contractes de confidencialitat amb els proveïdors de sistemes.

- **A nivell de la informació:**
  - Control d'accessos amb gestió d'autoritzacions.

- **A nivell dels equips d'usuari:**
  - Mesures de protecció contra codi maliciós
  - Gestió de privilegis
  - Accés VPN securitzat per accedir des de l'exterior de la xarxa

Motivació creació PDS

- Base fonamental per la **implantació d'un procés de millora contínua** (basat en el cicle de Deming) aplicat sobre la seguretat de la informació.

  - **Identificar i valorar els actius corporatius**
  - **Avaluar el corresponent anàlisi de riscos**
  - **Avaluar el nivell de compliment de la normativa referent a la seguretat de la informació en les organitzacions com és la ISO/IEC 27002:2005.**

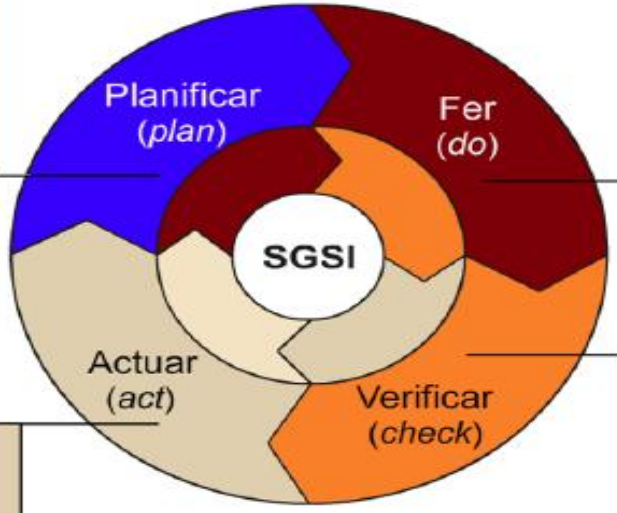
- Produirà un **coneixement de l'estat de la seguretat**; i permetrà plantejar les accions necessàries per **minimitzar el impacte dels riscos potencials** als quals es troba exposada l'organització.

Motivació creació PDS

Cicle de Deming aplicat als sistemes de gestió de seguretat de la informació

Establir l'SGSI

- P.I. Definir la política de seguretat
- P.II. Definir-ne l'abast
- P.III. Definir l'organització
- P.IV. Definir les polítiques d'alt nivell
- P.V. Definir els objectius de seguretat
- P.VI. Identificar els riscos
- P.VII. Seleccionar salvaguardes



Implantar i operar l'SGSI

- D.I. Implantar el pla de gestió del risc
- D.II. Seleccionar i implantar indicadors

Mantenir i millorar l'SGSI

- A.I. Implantar millores, accions preventives i preventives
- A.II. Mantenir registres

Monitorar i revisar l'SGSI

- C.I. Desenvolupar procediments de monitoratge
- C.II. Revisar regularment l'SGSI
- C.III. Auditar internament l'SGSI

Abast PDS

- ✓ Tots els **sistemes de la informació "concrets"** de l'organització que es trobem allotjats al CPD ES, **per oferir els diferents serveis.**

  (*Exclosos l'ERP de la companyia i la solució Futurmaster per trobar-se allotjada als CPD's Internacionals)*

- ✓ **Tots els sistemes bàsics** utilitzats a l'organització que presentin una infraestructura dintre de l'organització, **per oferir els diferents serveis.**

  (*Queden exclosos els sistemes Cloud o llicències d'ús a través d'internet on serà el proveïdor del servei l'encarregat de la seguretat d'aquest sistemes de la informació)*

- ✓ Totes **les instal·lacions que presenten relació** amb els sistemes de la informació de la societats, **per oferir els diferents serveis.**

- ✓ Tota **la infraestructura de comunicació** entre les diferents seus o amb els propis usuaris que es trobem utilitzant solucions considerades com "solucions Roaming". (anomenem aquestes solucions, a punts d'entrada de la informació als sistemes que es produeixen fora de la xarxa corporativa), **per oferir els diferents serveis.**

Abast PDS

- ✓ Infraestructura complerta dels diferents sistemes de la informació.

- ✓ Connexió i provisió de comunicació amb els sistemes externs.

El Resum de L'abast seria:

- ✓ **Serveis relacionats amb els sistemes de la informació proveïts des de el CPD ES cap a totes les seus de la Regió Ibèrica.**

  (E Indirectament de tots els actius i serveis relacionats per tal de poder oferir-los)

INDEX DE L'APARTAT

PRESENTACIÓ PLA DIRECTOR

- Necessitat del Pla Director
  - Beneficis
  - Impacte sobre l'organització
- Organització i seguiment del Pla Director
- Recursos pel Pla Director
  - Esponsorització del Pla
  - Recursos organitzatius
  - Recursos Materials
  - Sol·licitud de recursos

Necessitat del Pla Director

- Quin impacte te sobre l'organització la pèrdua de la base de dades de clients??
  - i de punts d'entrega o contactes?
  - o pot ser la pròpia informació de RRHH?

- Que procediment caldria seguir en cas de terratrèmol??
  - o altres tipus de fenòmens naturals?
  - estem preparats per afrontar-los?
- Quin valor tindria la pèrdua/parada del sistema de traçabilitat de producte terminat?
  - o de traçabilitat de matèries primes?

- Que s'ha de fer en cas de detectar una fuita de informació?
  - o personal no autoritzat a les instal·lacions?
- A quins riscos esta exposat ara mateix el sistema comercial??
  - Quin impacte tindríem?
  - Com evitar-ho?
  - Com prevenir-ho?

➢ Com veiem clarament, la realització d'aquest PDS ens permetrà poder **donar resposta a aquestes qüestions** i d'altres relacionades, i a la seva vegada ens permetrà **elevar el nostre nivell de seguretat entorn a la informació de l'organització** que avui dia es un actiu molt apreciat.

Beneficis del PDS

- ✓ **Normes de seguretat organitzatives.**
- ✓ **Pràctiques efectives** de gestió de la seguretat.
- ✓ Gestió i control sobre les relacions de informació amb **terceres organitzacions.**
- ✓ Complir les diferents conformitats a nivell de la **legislació i reglaments aplicables.**
- ✓ Assegurar que **els riscos de seguretat es gestionen** de manera efectiva en termes de costos.
- ✓ **Implementar i gestionar els controls** necessaris per a assegurar que s'aconsegueixen els objectius de seguretat que ha definit l'organització.
- ✓ **Conèixer el grau de compliment** de polítiques, directives i estàndards adoptats per l'organització, per part d'auditors interns o externs.
- ✓ **Establir polítiques, directives, estàndards o procediments de seguretat de la informació** en les relacions amb tercers.
- ✓ Convertir la seguretat de la informació en un **facilitador del negoci.**
- ✓ Proporcionar informació rellevant sobre **l'estat de la seguretat de la informació a clients.**

Impacte del PDS sobre l'organització

Nova filosofia de treball a l'organització:

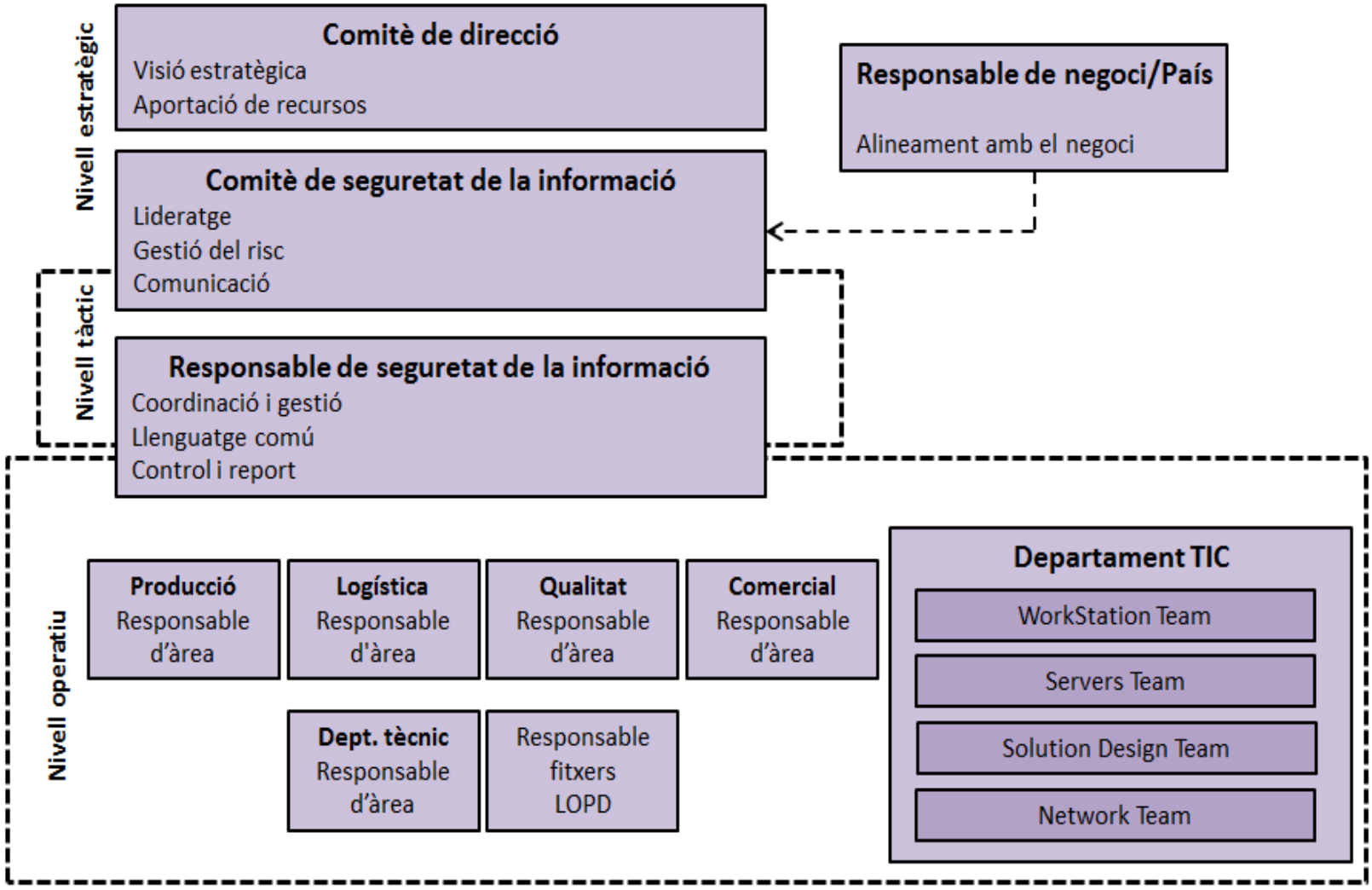
- Tractament de la seguretat de la informació
- Aplicació d'una metodologia de millora continua

Per tal d'obtenir aquest objectius finals, caldrà:

- Una carrega de treball extra per les noves tasques.
- Una nova metodologia de treball a seguir.
- Una transversalitat major entre els diferents departaments de l'organització i fonamentalment en coalició amb el departament de Sistemes de la informació.

PUNT NEGATIU→ hem de comentar que aquesta nova metodologia per realitzar les coses pot suposar **una pèrdua d'agilitat a costa d'incrementar la seguretat global.**

Organització pel Pla Director



Seguiment del Pla Director

El **responsable de seguretat de la informació**, realitzarà el seguiment de forma periòdica tant de l'evolució com del posterior manteniment i millora constant un cop establert.

Per garantir el seguiment, durant el desenvolupament s'estableixen 4 fases clares:

- **FASE 1: Confecció de l'anàlisi de Riscos.**
- **FASE 2: Auditoria de compliment de la ISO/IEC 27002:2005**
- **FASE 3: Proposició de Projectes**
- **FASE 4: Implantació dels projectes acceptats.**

Durant les 4 fases, es prepararan uns **informes a completar amb l'evolució de la fase, els possibles problemes i els pròxims passos** a efectuar que serà **presentat al comitè de seguretat** establert.

- **Document establert de seguiment i revisió de l'evolució de la fase.**

De cara a la implantació del projectes, **el seguiment es realitzarà de forma individual per cada projecte,** per tal de **reduir les possibles desviacions tant temporals com econòmiques.**

- **Document establert de seguiment i revisió per cada projecte.**

Temporalment s'estableixen **tres controls mínims → Inici - Meitat - Finalització**

Esponsorització del Pla

Donada **la transversalitat i la implicació** de tots els col·laboradors de l'organització, ***resulta imperatiu*** que la Direcció realitzi:

- **Validació de la confecció del PDS**
- **Assignació de recursos necessaris per la confecció**
- **Assignació de recursos per l'evolució posterior**
- **Validació de la estructura organitzativa de gestió per la seguretat de la informació**

- **Comunicació i presentació a tota l'organització del l'inici de la confecció del pla com de la importància dels objectius assolir**
- **Implicar i motivar a tot el personal involucrat en el PDS**

INDEX DE L'APARTAT

ESTAT DEL RISC

- Metodologia seguida
- Inventari d'actius
- Valoració d'actius
- Dimensions de seguretat
- Taula Resultat Valoració
- Anàlisis d'amenaces
- Impacte Potencial
- Resum Objectius Assolits amb l'anàlisi de Riscos

Metodologia seguida

- Per tal de realitzar l'anàlisi de Riscos de l'organització, hem decidit seguir la **Metodologia de MAGERIT** per tal de poder obtenir:

  - Una **anàlisi detallada dels actius** rellevants a nivell de seguretat per a l'empresa.
  - Un **estudi de les possibles amenaces** sobre els sistemes d'informació, així com quin seria el seu impacte en la mateixa.
  - Una **avaluació del impacte potencial** que tindria la materialització de les diferents amenaces a què estan exposades els nostres actius.

Inventari d'actius

Tal com s'indica a **la guia de MAGERIT,** hem classificat els actius, **en funció del seu àmbit**, en els següents grups:

- **Instal·lacions [L]**
- **Hardware [HW]**
- **Aplicació [SW]**
- **Dades / Informació [D]**
- **Xarxa / Comunicacions [COM]**
- **Serveis [S]**
- **Suports de Informació [SI]**
- **Equipament auxiliar [AUX]**
- **Personal [P]**

En la memòria d'aquest TFM podem observar **la taula complerta d'actius i les dependències que existeixen entre ells.**

DEPENDENCIA ENTRE ACTIUS: *Un "actiu superior" depèn d'un altre "actiu inferior" quan les necessitats de seguretat del superior es reflecteixen en les necessitats de seguretat de l'inferior.*

Valoració d'actius

Càlcul del valor d'un actiu → **Tasca Complicada**

- *Valor reposició + valor info. + ... + penalització + ...+*
  ("Tot una sèrie de costos imputables a l'actiu")

➢ De cara a facilitar la tasca, seguint la recomanació de MAGERIT i preparem una **taula de equivalència** entre **valor qualitatiu i quantitatiu** pels nostres actius.

VALORACIO	RANG	VALOR
Molt Alta (MA)	Valor > 200K€	300K€
Alta (A)	100k€ < Valor < 200k€	150K€
Mitjana (M)	50k€ < Valor < 100K€	75k€
Baixa (B)	10k€ < Valor < 50K€	30k€
Molt Baixa (MB)	Valor < 10k€	10k€

Dimensions de seguretat

- **[C] Confidencialitat.** Només les persones autoritzades tenen accés a la informació sensible o privada.
- **[I] Integritat.** La informació i els mètodes de processament d'aquesta informació són exactes i complets, i no s'han de manipular sense autorització.
- **[D] Disponibilitat.** Els usuaris que hi estan autoritzats podem accedir a la informació quan ho necessitin.
- **[A] Autenticitat.** Hi ha garantia de la identitat dels usuaris o processos que tracten la informació.
- **[T] No Repudi.** Hi ha garantia de l'autoria d'una determinada acció i esta associat qui o que a produït aquesta acció.

VALOR	CRITERIO
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	Irrellevant per la organització

Exemple Taula Resultat Valoració

(Exemple del contingut → Taula sencera a la memòria del TFM)

ÀMBIT	ACTIU		DEPENDÈNCIA	VALOR	ASPECTES CRÍTICS				
					C	I	D	A	T
[L] - Instal.lacions	[L.1]	CPD ES		MA	8	9	10	9	9
	[L.3]	Sala comunicacions HQ PT		A	8	8	10	9	8
[HW] - Hardware	[HW.1]	Servidor Correu [ESWK3MAD02]	[L.1] - [HW.2] - [HW.3] [HW.4] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [D.13]	MB	8	7	8	6	6
	[HW.12]	Servidor Web [SRVMAD23]	[L.1] - [HW.21] - [HW.9] [COM.1] - [COM.2] - [COM.3] [COM.4] - [D.16]	B	8	8	9	6	6
	[HW.13]	Servidor Distrib. Aplicacions [SRVMAD30]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4]	MB					
	[HW.21]	Switches LAN CPD	[L.1]	MB	8	9	10	9	9
	[HW.27]	Terminals Lectura SGANL	[HW.24] - [HW.25] - [HW.26]	B	5	7	8	5	5
	[HW.30]	Acces Points INFOLOG	[HW.24] - [HW.25] - [HW.26]	B	5	8	10	7	5
[SW] - Aplicació	[SW.1]	Aplicació SKEP	[HW.16]	B	5	9	7	7	5
	[SW.2]	Aplicació INFOLOG	[HW.17] - [HW.18]	MA	5	8	10	7	5
[D] - Dades/Info.	[D.1]	Dades propies Intranet	[SI.1] - [HW.9]	M	8	8	6	9	7
	[D.12]	Dades CALOR	[SI.18] - [SI.19] - [HW.20] - [SW.6]	MA	6	8	10	8	8
	[D.14]	Dades FileServer HQ ES	[SI.4] - [HW.5]	A	6	8	7	4	4
[COM] - Xarxa	[COM.1]	Router Primari CPD ES	[L.1]	MB	8	9	10	9	9
	[COM.2]	Línia Principal CPD ES	[L.1]	MB	8	9	10	9	9
[S] - Serveis	[S.1]	Servei de Correu Usuaris	[HW.1] - [HW.2]	M	8	7	8	6	6
	[S.15]	Servei FUTURMASTER	[COM.5] - [COM.6] - [COM.7] [COM.8] - [COM].9] - [COM.10] [COM.11] - [COM.12]	M					
	[S.16]	Servei PRISMA	[SW.4]	B	3	7	4	3	3
	[S.17]	Servei ORALIMS	[SW.5]	M	7	9	8	9	9
[SI] - Suports de Informació	[SI.1]	Cabina de Discos [ESNAS01]	[D.1] - [D.2] - [D.3] - [D.4] - [D-5] [D.16]	B	8	8	9	9	7
	[SI.18]	Discos Server [SRVMAD06]	[D.6] - [D.8] - [D.9] - [D.10] [HW.19]	MB	7	9	8	9	9
	[SI.19]	Discos Server [SRVMAD07]	[D.12] - [HW.20]	MB	6	8	10	8	8
[AUX] - Equipament auxiliar	[AUX.1]	UPS pel CPD	[L.1]	M	8	9	10	9	9
	[AUX.2]	Equip climatització CPD	[L.1]	B	8	9	10	9	9
	[AUX.16]	UPS CD PT	[L.6]	MB	5	8	10	7	5
[P] - Personal	[P.1]	Responsable de Seguretat		M					
	[P.9]	Responsable Bases de Dades		B					

Valoració Serveis

ÀMBIT	ACTIU (id)	ACTIU	DEPENDÈNCIA	VALOR	ASPECTES CRÍTICS				
					C	I	D	A	T
[S] - Serveis	[S.1]	Servei de Correu Usuaris	[HW.1] - [HW.2]	M	8	7	8	6	6
	[S.2]	Servei Comunicació Interna	[HW.7] - [HW.8]	M					
	[S.3]	Servei Intranet	[HW.9]	M	8	8	6	9	7
	[S.4]	Servei Web Marca [X]	[HW.9]	B	6	7	5	4	4
	[S.5]	Servei Web Marca [Y]	[HW.9]	B	6	7	5	4	4
	[S.6]	Servei Web Marca [Z]	[HW.9]	B	6	7	5	4	4
	[S.7]	Servei Web Promoció [2X]	[HW.9]	B	6	7	5	4	4
	[S.8]	Provisió Antivirus Usuaris	[HW.14]	B					
	[S.9]	Servei Firewall	[HW.15]	A					
	[S.10]	Servei SKEP	[SW.1]	B	5	9	7	7	5
	[S.11]	Servei Intercanvi de Fitxers	[HW.16]	MB	3	3	4	2	2
	[S.12]	Servei INFOLOG	[SW.2]	MA	5	8	10	7	5
	[S.13]	Servei SGANL	[SW.3]	B	5	7	8	5	5
	[S.14]	Servei SAP	[COM.13] - [COM.14] - [COM.15] [COM.16]	MA					
	[S.15]	Servei FUTURMASTER	[COM.5] - [COM.6] - [COM.7] [COM.8] - [COM].9] - [COM.10] [COM.11] - [COM.12]	M					
	[S.16]	Servei PRISMA	[SW.4]	B	3	7	4	3	3
	[S.17]	Servei ORALIMS	[SW.5]	M	7	9	8	9	9
	[S.18]	Servei CALOR	[SW.6]	MA	6	8	10	8	8
	[S.19]	Servei Accés VPN	[HW.15]	B					
	[S.20]	Servei FileServer ES	[HW.5]	M	6	8	7	4	4
	[S.21]	Servei FileServer PT	[HW.6]	M	6	8	7	4	4

Anàlisis d'amenaces

De cara a poder implementar la anàlisi d'amenaces a les quals estan exposats els nostres actius, serà important valorar:

- **Freqüència d'ocurrència**

VALORACIO	FREQÜÈNCIA	VALOR CÀLCUL
Freqüència Extrema (FE)	1 vegada al dia	1
Freqüència Alta (FA)	1 vegada cada 2 setmanes	26/365
Freqüència Mitjana (FM)	1 vegada cada 2 mesos	6/365
Freqüència Baixa (FB)	1 vegada cada 6 mesos	2/365
Freqüència molt Baixa(FMB)	1 vegada any (o menys)	1/365

- **Impacte** sobre l'organització en cas de materialització

IMPACTE	VALOR
Molt Alt (MA)	100%
Alt (A)	75%
Mitjà (M)	50%
Baix (B)	20%
Molt Baix (MB)	5%

- En funció de l'àmbit de l'actiu; **MAGERIT defineix a quines amenaces es pot veure exposat.**

  - **(Utilització de la nomenclatura definida a la metodologia MAGERIT en el seu volum 2 – Catàleg d'elements)**

Amenaces sobre un actiu de tipus Servei

ACTIU/AMENACES		FREQÜÈNCIA (X/365)	IMPACTE				
			C	I	D	A	T
Servei SKEP			35%	50%	85%	15%	25%
Errors d'usuari	[E.1]	25	0%	35%	5%	0%	0%
Errors dels Administradors	[E.2]	5	15%	50%	25%	5%	25%
Errors de monitorització (log)	[E.3]	1	0%	0%	0%	0%	1%
Errors de configuració	[E.4]	10	25%	45%	15%	15%	5%
Errors de [re-]encaminament	[E.9]	0	0%	0%	0%	0%	0%
Errors de seqüencia	[E.10]	0	0%	0%	0%	0%	0%
Parada del sistema per agotament dels recursos	[E.24]	3	0%	0%	85%	0%	0%
Manipulació de la configuració	[A.4]	1	35%	50%	75%	15%	20%
Suplantació de la identitat de l'usuari	[A.5]	1	25%	25%	0%	15%	0%
Aprofitament dels privilegis d'accés	[A.6]	3	35%	45%	0%	0%	0%
Usos no previstos	[A.7]	5	0%	0%	70%	0%	0%
[Re-]encaminament de missatges	[A.9]	0	0%	0%	0%	0%	0%
Alteració de la seqüencia	[A.10]	0	0%	0%	0%	0%	0%
Accessos no autoritzats	[A.11]	1	25%	35%	0%	5%	0%
Repudi	[A.13]	1	0%	0%	0%	0%	25%
Denegació de servei	[A.24]	1	0%	0%	50%	0%	0%

(Exemple del contingut → Taula sencera a la memòria del TFM)

Impacte Potencial

IP = Valor Actiu(per Dimensió) x Impacte (degradació que causa)

ACTIU	Valoració					IMPACTE					IMPACTE POTENCIAL				
	C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
Servei de Correu Usuaris	8	7	8	6	6	**85%**	**75%**	**100%**	**65%**	**85%**	6,80	5,25	8,00	3,90	5,10
Servei Intranet	8	8	6	9	7	75%	75%	100%	50%	35%	6,00	6,00	6,00	4,50	2,45
Servei Web Marca [X]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
Servei Web Marca [Y]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
Servei Web Marca [Z]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
Servei Web Promoció [2X]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
Servei SKEP	5	9	7	7	5	35%	50%	85%	15%	25%	1,75	4,50	5,95	1,05	1,25
Servei Intercanvi de Fitxers	3	3	4	2	2	50%	25%	85%	50%	30%	1,50	0,75	3,40	1,00	0,60
Servei INFOLOG	5	8	10	7	5	50%	45%	50%	25%	25%	2,50	3,60	5,00	1,75	1,25
Servei SGANL	5	7	8	5	5	35%	50%	75%	15%	25%	1,75	3,50	6,00	0,75	1,25
Servei PRISMA	3	7	4	3	3	35%	50%	75%	15%	25%	1,05	3,50	3,00	0,45	0,75
Servei ORALIMS	7	9	8	9	9	35%	65%	75%	15%	25%	2,45	5,85	6,00	1,35	2,25
Servei CALOR	6	8	10	8	8	50%	50%	95%	25%	25%	3,00	4,00	9,50	2,00	2,00
Servei FileServer ES	6	8	7	4	4	50%	30%	85%	35%	25%	3,00	2,40	5,95	1,40	1,00
Servei FileServer PT	6	8	7	4	4	50%	30%	85%	35%	25%	3,00	2,40	5,95	1,40	1,00

Resum Objectius Assolits amb l'Anàlisi de Riscos

- Una **anàlisi detallada dels actius** rellevants a nivell de seguretat per a l'empresa.
- Un estudi de **les possibles amenaces** sobre el S.I. (amb el seu impacte sobre l'empresa)

- Una **avaluació del impacte potencial que tindria la materialització** de les diferents amenaces a què estan exposades els nostres actius.

INDEX DE L'APARTAT

AUDITORIA COMPLIMENT ISO

- Metodologia a seguir
- Avaluació de la maduresa
- Presentació de resultats
  - Resultats per Domini
  - Resultats de la Maduresa
  - Resultats respecte el Target definit per l'organització
- Resum Objectius de l'auditoria

Metodologia a seguir

L'estàndard ISO / IEC 27002:2005, agrupa un total de **133 controls o salvaguardes** sobre bones pràctiques per a la Gestió de la Seguretat de la Informació organitzat en **11 àrees i 39 objectius de control**. Aquest estàndard és internacionalment reconegut i és perfectament vàlid per la majoria d'organitzacions.

Hi ha diferents aspectes en els quals les salvaguardes actuen reduint el risc, ja parlem dels controls ISO / IEC 27002:2005 o de qualsevol altre catàleg. Aquests són en general:

- Formalització de les pràctiques mitjançant documents escrits o aprovats.
- Política de personal.
- Sol·licituds tècniques (programari, maquinari o comunicacions).
- Seguretat física.

La protecció integral davant les possibles amenaces, requereix d'una combinació de salvaguardes sobre cada un d'aquests aspectes.

Avaluació de la maduresa

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	**Inexistent**	Manca completa de qualsevol procés recognoscible. No s'ha reconegut si més no que hi ha un problema a resoldre.
10%	L1	**Inicial / Ad-hoc**	Estat inicial on l'èxit de les activitats dels processos es basa la majoria de les vegades en l'esforç personal. Els procediments són inexistents o localitzats en àrees concretes. No hi ha plantilles definides a nivell corporatiu.
50%	L2	**Reproduïble, però intuïtiu**	Els processos similars es porten en forma similar per diferents persones amb la mateixa tasca. Es normalitzen les bones pràctiques sobre la base de l'experiència i al mètode. No hi ha comunicació o entrenament formal, les responsabilitats a càrrec de cada individu. Es depèn del grau de coneixement de cada individu.
90%	L3	**Procés definit**	L'organització sencera participa en el procés. Els processos estan implantats, documentats i comunicats mitjançant entrenament.
95%	L4	**Gestionat i mesurable**	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos. Es disposa de tecnologia per automatitzar el flux de treball, es tenen eines per millorar la qualitat i l'eficiència.
100%	L5	**Optimitzat**	Els processos estan sota constant millora. En base a criteris quantitatius es determinen les desviacions més comuns i s'optimitzen els processos.

Resultats per Domini

CONTROL	Situació
5. POLÍTICA DE SEGURETAT	**28%**
5.1 Política de seguretat de la informació	28%
5.1.1 Document de política de seguretat de la informació	40%
5.1.2 Revisió de la política de seguretat de la informació	15%
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ	**45%**
6.1 Organització Interna	28%
6.1.1 Compromís de la Direcció amb la seguretat de la informació	60%
6.1.2 Coordinació de la seguretat de la informació	25%
6.1.3 Assignació de responsabilitats relatives a la seguretat de la Informació	15%
6.1.4 Procés d'autorització de recursos per el tractament de la Informació	25%
6.1.5 Acords de confidencialitat	60%
6.1.6 Contacte amb les autoritats	20%
6.1.7 Contacte amb grups d'especial interès	10%
6.1.8 revisió independent de la seguretat de la informació	5%
6.2 Tercers	62%
6.2.1 Identificació dels riscos derivats dels accessos de tercers	**50%**
6.2.2 Tractament de la seguretat en la relació amb els clients	**70%**
6.2.3 Tractament de la seguretat en contractes amb tercers	**65%**
7. GESTIÓ D'ACTIUS	**57%**
7.1 Responsabilitat sobre els actius	92%
7.1.1 Inventari d'actius	85%
7.1.2 Propietat dels actius	100%
7.1.3 Us acceptable dels actius	90%
7.2 Classificació de la informació	23%
7.2.1 Directrius de la classificació	25%
7.2.2 Etiquetatge i manipulació de la informació	20%

Resultats per Domini

8. SEGURETAT LLIGADA ALS RECURSOS HUMANS	**70%**
8.1 Abans del treball	62%
8.1.1 Funcions i responsabilitats	65%
8.1.2 Investigació d'antecedents	35%
8.1.3 Termes i condicions de contractació	85%
8.2 Durant el treball	57%
8.2.1 Responsabilitats de la Direcció	75%
8.2.2 Conscienciació, formació i capacitació en seg. De la informació	30%
8.2.3 Processos disciplinaris.	65%
8.3 Finalització del treball o canvi de posició de treball	92%
8.3.1 Responsabilitats de finalització o canvi	80%
8.3.2 Devolució d'actius	100%
8.3.3 Retirada dels drets d'accés	95%
9. SEGURETAT FÍSICA I DEL ENTORN	**85%**
9.1 Àrees segures	74%
9.1.1 Perímetre de seguretat física	60%
9.1.2 Controls físics d'entrada	30%
9.1.3 Seguretat d'oficina, despatxos e instal·lacions	85%
9.1.4 Protecció contra les amenaces externes i d'origen ambiental	90%
9.1.5 Treball en àrees segures	85%
9.1.6 Àrees d'accés públic i de carrega i descàrrega	95%
9.2 Seguretat dels equips	96%
9.2.1 Localització i protecció dels equips	95%
9.2.2 Instal·lacions de subministrament	95%
9.2.3 Seguretat del cablatge	95%
9.2.4 Manteniment dels equips	95%
9.2.5 Seguretat dels equips fora de les instal·lacions	95%
9.2.6 Reutilització o retirada segura dels equips	95%
9.2.7 Retirada de materials propietat de l'empresa	100%

Resultats per Domini

10. GESTIÓ DE COMUNICACIONS I OPERACIONS	59%
10.1 Responsabilitats i procediments d'operació	34%
10.1.1 Documentació dels procediments d'operació	60%
10.1.2 Gestió de canvis	25%
10.1.3 Segregació de tasques	35%
10.1.4 Separació dels recursos de desenvolupament, prova i operació	15%
10.2 Gestió de la provisió de serveis per tercers	78%
10.2.1 Provisió de serveis	95%
10.2.2 Supervisió i revisió dels serveis prestats per tercers	75%
10.2.3 Gestió del canvi en els serveis prestats per tercers	65%
10.3 Planificació i acceptació del sistema	33%
10.3.1 Gestió de capacitats	35%
10.3.2 Acceptació del sistema	30%
10.4 Protecció davant codi maliciós i descarregable	88%
10.4.1 Controls contra codi maliciós	80%
10.4.2 Controls contra codi descarregable en el client	95%
10.5 Copies de Seguretat	95%
10.5.1 Copies de seguretat de la informació	95%
10.6 Gestió de la seguretat de les xarxes	55%
10.6.1 Controls de xarxa	45%
10.6.2 Seguretat dels serveis de xarxa	65%
10.7 manipulació dels suports	73%
10.7.1 Gestió de suports extraibles	75%
10.7.2 Retirada de suports	85%
10.7.3 Procediment de manipulació de la informació	75%
10.7.4 Seguretat de la documentació del sistema	55%

Resultats per Domini

10.8 Intercanvi de informació	**59%**
10.8.1 Política i procediment de intercanvi de informació	60%
10.8.2 Acord de intercanvi	40%
10.8.3 Suport físic en transit	35%
10.8.4 Missatgeria electrònica	75%
10.8.5 Sistemes de informació empresarials	85%
10.9 Serveis de comerç electrònic	N/A
10.9.1 Comerç electrònic	N/A
10.9.2 Transaccions en línia	N/A
10.9.3 Informació públicament disponible	N/A
10.10 Supervisió	15%
10.10.1 Registres d'auditories	20%
10.10.2 Supervisió del us del sistema	25%
10.10.3 Protecció de la informació dels registres	15%
10.10.4 Registres d'administració i operació	10%
10.10.5 Registres de fallades	10%
10.10.6 Sincronització del rellotge	10%
11. CONTROL D'ACCESSOS	**76%**
11.1 Requisits de negociació pel control d'accessos	75%
11.1.1 Política de control d'accessos	75%
11.2 Gestió d'accessos d'usuari	78%
11.2.1 Registre d'usuari	85%
11.2.2 Gestió de privilegis	95%
11.2.3 Gestió de contrasenyes d'usuari	85%
11.2.4 Revisió dels drets d'accés d'usuari	45%
11.3 Responsabilitats d'usuari	57%
11.3.1 Us de contrasenyes	85%
11.3.2 Equip d'usuari desatès	50%
11.3.3 Política d'estació de treball net i pantalla neta	35%

Resultats per Domini

11.4 Control d'accés a la xarxa	**81%**
11.4.1 Política d'us dels serveis en xarxa	95%
11.4.2 Autenticació d'usuaris per connexions externes	100%
11.4.3 Identificació dels equips en les xarxes	90%
11.4.4 Protecció dels port de diagnosis i configuracions remotes	25%
11.4.5 Segregació de xarxes	65%
11.4.6 Control de la connexió de xarxa	95%
11.4.7 Control d'encaminament(Routing) de xarxa	100%
11.5 Control d'accés al sistema operatiu	91%
11.5.1 Procediments segurs d'inici de sessió	95%
11.5.2 Identificació i autenticació d'usuari	100%
11.5.3 Sistema de gestió de contrasenyes	100%
11.5.4 Us dels recursos del sistema	95%
11.5.5 Desconnexió automàtica de sessió	65%
11.5.6 Limitació del temps de connexió	90%
11.6 Control d'accés a les aplicacions i a la informació	98%
11.6.1 Restricció del accés a la informació	95%
11.6.2 Aïllament de sistemes sensibles	100%
11.7 Ordinadors portables i teletreball	53%
11.7.1 Ordenadors portables i comunicacions mòbils	60%
11.7.2 Teletreball	45%

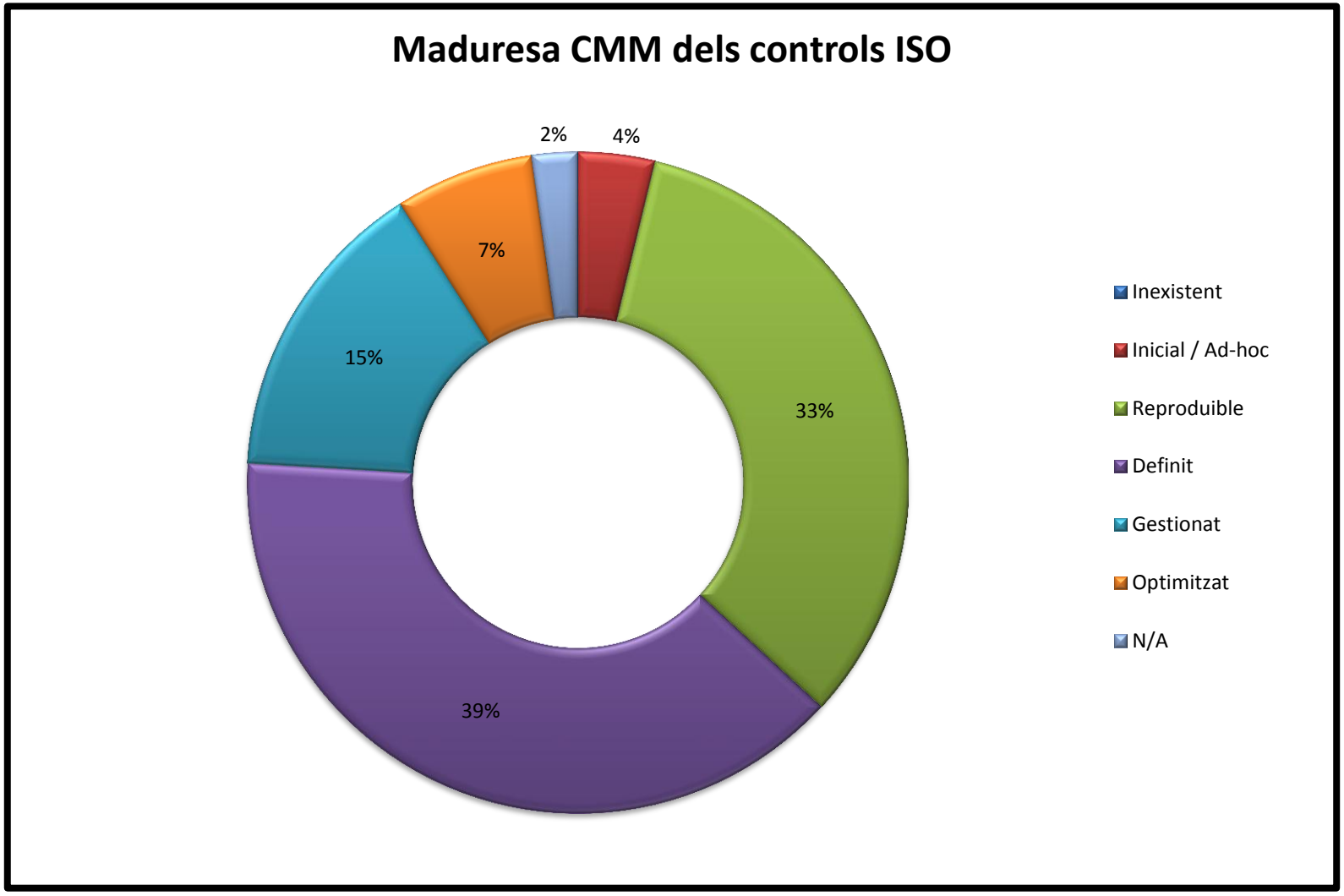
Resultats per Domini

12. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DE S.I.	**68%**
12.1 Requisits de seguretat dels sistemes de informació	70%
12.1.1 Anàlisi i especificacions dels requeriments de seguretat	70%
12.2 Tractament correcte de les aplicacions	86%
12.2.1 Validació de les dades d'entrega	85%
12.2.2 Control del processament intern	90%
12.2.3 Integritat dels missatges	80%
12.2.4 Validació de les dades de sortida	90%
12.3 Controls criptogràfics	65%
12.3.1 Política d'us dels controls criptogràfics	35%
12.3.2 Gestió de claus	95%
12.4 Seguretat dels arxius de sistema	95%
12.4.1 Control del software en explotació	90%
12.4.2 Protecció de les dades de prova del sistema	95%
12.4.3 Control d'accés al codi font dels programes	100%
12.5 Seguretat en els processos de desenvolupament i suport	56%
12.5.1 Procediment de control de canvis	35%
12.5.2 Revisió tècnica aplicacions després d'efectuar canvis al S.O.	35%
12.5.3 Restriccions als canvis en els paquets de software	85%
12.5.4 Fuites de informació	40%
12.5.5 Externalització del desenvolupament de soft.	85%
12.6 Gestió de la vulnerabilitat tècnica	35%
12.6.1 Control de les vulnerabilitats tècniques	35%
13. GESTIÓ D'INCIDENTS EN LA SEGURETAT DE LA INFORMACIÓ	**41%**
13.1 Notificació d'events i punts febles de seguretat de la informació	48%
13.1.1 Notificació dels successos de seguretat de la informació	60%
13.1.2 Notificació dels punts febles de seguretat	35%
13.2 Gestió d'incidents i millores de seguretat de la informació	35%
13.2.1 Responsabilitats i procediments	45%
13.2.2 Aprenentatge dels incidents de S.I.	45%
13.2.3 Recopilació d'evidències	15%

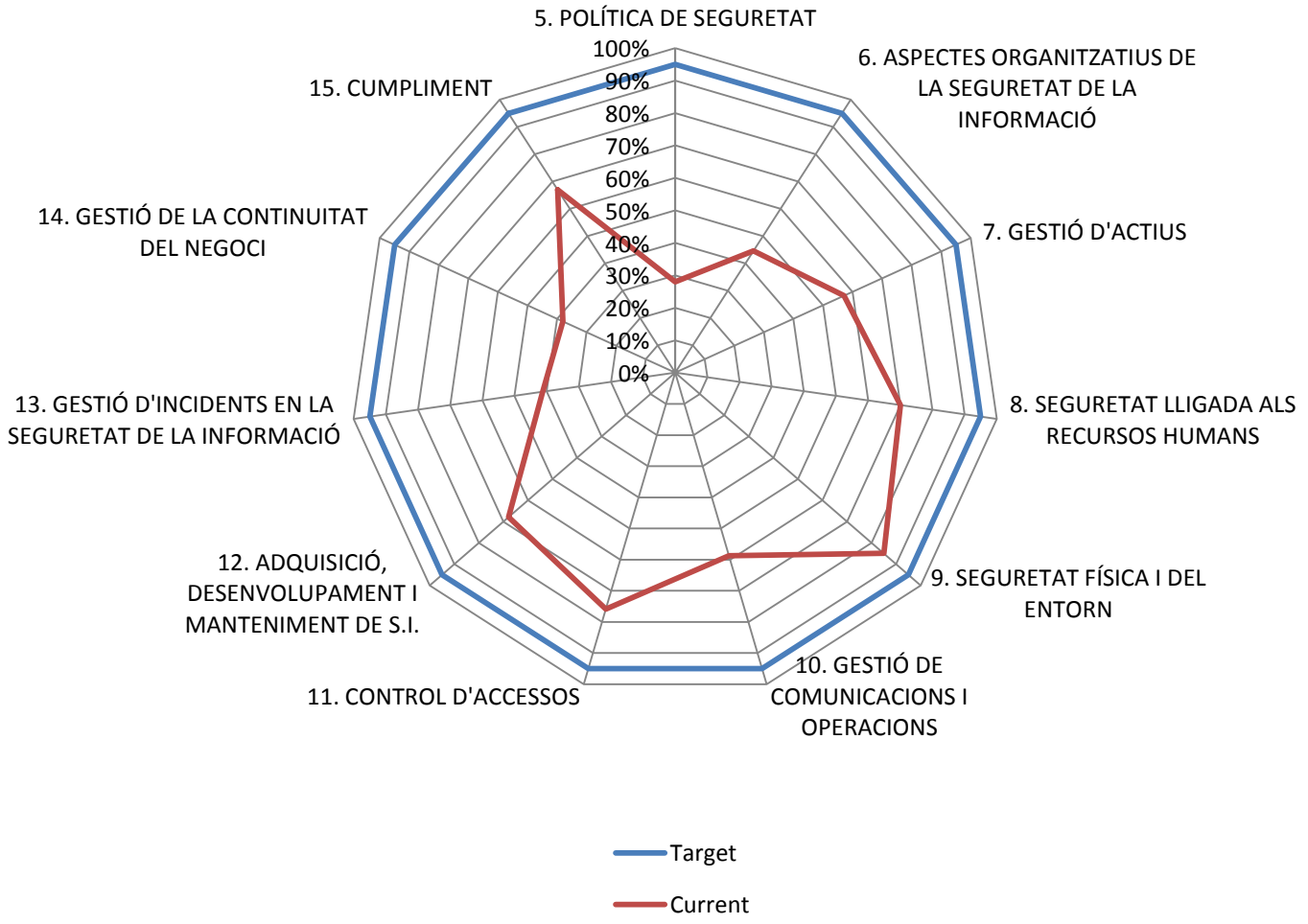
Resultats per Domini

14. GESTIÓ DE LA CONTINUITAT DEL NEGOCI	**38%**
14.1 Aspectes de seguretat de la informació en la gestió de la continuïtat del negoci	38%
14.1.1 Inclusió de la seguretat de la informació en el procés de gestió de la continuïtat del negoci	25%
14.1.2 Continuïtat del negoci i avaluació de riscos	65%
14.1.3 Desenvolupament e implantació de plans de continuïtat que incorporin la S.I.	40%
14.1.4 Marc de referencia per la planificació de la cont. Del negoci	45%
14.1.5 Proves, manteniment i revaluació de plans de continuïtat	15%
15. CUMPLIMENT	**67%**
15.1 Compliment dels requisits legals	68%
15.1.1 Identificació de la legislació aplicable	85%
15.1.2 Drets de propietat intel·lectual (DPI)	85%
15.1.3 Protecció dels documents de la organització	90%
15.1.4 Protecció de dades i privacitat de la informació de caràcter personal	95%
15.1.5 Prevenció de l'ús inadequat de recursos de tractament de la informació	25%
15.1.6 Regulació dels controls criptogràfics	30%
15.2 Compliment de les polítiques i normes de seguretat i compliment tècnic	73%
15.2.1 Compliment de les polítiques i normes de seguretat	80%
15.2.2 Comprovació del compliment tècnic	65%
15.3 Consideracions sobre les auditories dels sistem. De la informació	60%
15.3.1 Controls d'auditoria dels sistemes de informació	35%
15.3.2 Protecció de les eines d'auditoria dels sistemes de informació	85%

Resultats de la Maduresa



Resultats respecte el Target definit per l'organització



Resum Objectius de l'auditoria

Un cop finalitzada aquesta fase, estem en disposició de:

- Una **visió del compliment dels diferents capítols de la ISO/IEC 27002:2005** – i del seu incompliment-.

- Una **auditoria interna complerta inicial** de la situació.
- Uns **registres de l'auditoria** per fonamentar les decisions futures.

INDEX DE L'APARTAT

PROPOSTES DE MILLORES

- Llistat de millores / Projectes a implementar
- Tractament Global Iniciatives
  - Planificació temporal integrada al PDS
  - Planificació econòmica integrada al PDS
- Anàlisi d'impacte dels projectes sobre la seguretat de la informació
  - Evolució Risc / Impacte Potencial
  - Evolució Nivell Compliment ISO
- Canvis Organitzatius conseqüència del PDS
- Resum Objectius assolits amb les iniciatives

Llistat de millores / Projectes a implementar

ID. PROJ.	NOM DEL PROJECTE	TEMPS	PRESSUPOST
PRO/TEC - 001	Virtualització Plena	3 mesos	200k€
PRO/TEC - 002	Organització FTP Secure	20 dies	2,5k€
PRO/TEC - 003	Seguretat perimetral Xarxa	20 dies	13,5k€
INI/DOC - 001	Creació BCP	6 mesos	Capex: 280k€ Opex: 50k€
INI/DOC - 002	Creació Document Seguretat	1 mes	4,4k€
PRO/TEC - 004	Sistema de monitorització Xarxa	2 mesos	5k€
INI/DOC - 003	Classificació de la informació	2 mesos	3k€
INI/PROC - 001	Depuració Inventari Actius	14 dies	0,5k€
INI/PROC - 002	Tractament de la informació de RRHH	1 mes	2k€
INI/ORG - 001	Consolidació comitè de Seguretat/Salut	1 mes	3k€
INI/PROC - 003	Coordinació en la gestió de canvis	2,5 mesos	5k€
INI/DOC - 004	Definició Requeriments Sistemes	14 dies	1,5k€
INI/PROC - 004	Gestió Backup informació	1 mes	3k€
INI/DOC - 005	Revisió politica control d'accessos	20 dies	2,5k€
INI/DOC - 006	Política de manteniment dels S.I.	2 mesos	6k€
INI/PROC - 005	Tractament de la gestió d'incidents en la S.I.	2 mesos	8k€
INI/AUDIT - 001	Control de compliment dels procediments/normes i requeriments legals	1 mes	4k€

Planificació temporal integrada al PDS

	Temps	Pressupost	Pre-Requisit	Any 2013	Any 2014	Any 2015	Any 2016
PRO/TEC - 001	3 mesos	200k€					
PRO/TEC - 002	20 dies	2,5k€	PRO/TEC - 001				
PRO/TEC - 003	20 dies	13,5k€					
INI/DOC - 001	6 mesos	Capex: 280k€ Opex: 50k€					
INI/DOC - 002	1 mes	4,4k€					
PRO/TEC - 004	2 mesos	5k€	PRO/TEC - 001 PRO/TEC - 003				
INI/DOC - 003	2 mesos	3k€	INI/DOC - 002				
INI/PROC - 001	14 dies	0,5k€					
INI/PROC - 002	1 mes	2k€					
INI/ORG - 001	1 mes	3k€					
INI/PROC - 003	2,5 mesos	5k€					
INI/DOC - 004	14 dies	1,5k€					
INI/PROC - 004	1 mes	3k€					
INI/DOC - 005	20 dies	2,5k€	INI/DOC - 002				
INI/DOC - 006	2 mesos	6k€					
INI/PROC - 005	2 mesos	8k€					
INI/AUDIT - 001	1 mes	4k€	INI/DOC - 002				

Planificació econòmica integrada al PDS

- **Pes Principal del cost econòmic** → Primers 2 anys del pla

- **El projectes d'indole tècnica** son els que presenten **major despeses i estan situats als primers anys de la planificació** d'aquest PDS, de cara a poder **establir un cicle de vida del serveis.**

- **La confecció del Business Continuity Plan (BCP)**, incorporarà un **cost recurrent anual de cara al manteniment de la solució** preparada per l'organització.

ANY	COST
2013	226K€
2014	296K€
2015	19K€ (+50K€ Opex)
2016	4k€ (+50k€ Opex)
TOTAL	**545 K€ (50K€ Opex per Any)**

Anàlisi d'impacte dels projectes sobre la seguretat de la informació

- **Virtualització Plena (PRO/TEC – 001)**
  - Millora resultats observats A.R.
- **Organització FTP Secure (PRO/TEC – 002)**
  - Millora resultats observats A.R.
- **Seguretat perimetral Xarxa (PRO/TEC – 003)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Objectiu de control 10.4 i 10.6
- **Creació BCP (INI/DOC – 001)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Domini 14
- **Creació Document Seguretat (INI/DOC – 002)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Domini 5 i 6
  - Objectiu de control 11.1 i 15.1
- **Sistema de monitorització Xarxa (PRO/TEC – 004)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Objectiu de control 10.10

Anàlisi d'impacte dels projectes sobre la seguretat de la informació

- **Classificació de la informació (INI/DOC – 003)**
  - Focalitzat sobre Domini 7
  - Focalitzat sobre Objectiu de control 10.8
- **Depuració Inventari Actius (INI/PROC – 001)**
  - Focalitzat sobre Domini 7
- **Tractament de la informació de RRHH (INI/PROC – 002)**
  - Focalitzat sobre Domini 8
- **Consolidació comitè de Seguretat/Salut (INI/ORG – 001)**
  - Focalitzat sobre Domini 9
- **Coordinació en la gestió de canvis (INI/PROC – 003)**
  - Focalitzat sobre Objectiu de control 10.1 i 10.2
- **Definició Requeriments Sistemes (INI/DOC – 004)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Objectiu de control 10.3

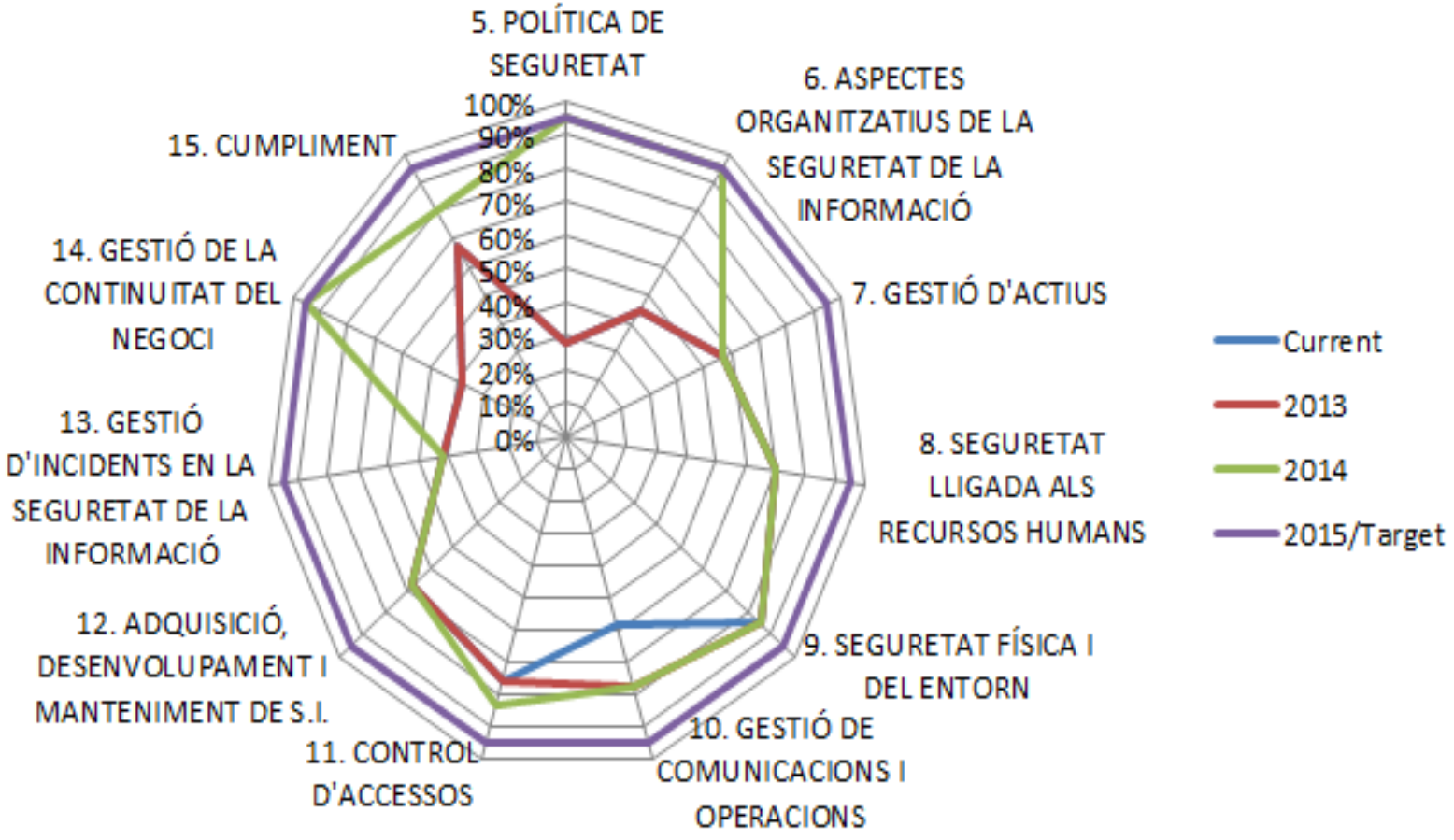
Anàlisi d'impacte dels projectes sobre la seguretat de la informació

- **Gestió Backup informació (INI/PROC – 004)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Objectiu de control 10.7
- **Revisió política control d'accessos (INI/DOC – 005)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Domini 11
  - Focalitzat sobre Objectiu de control 15.1
- **Política de manteniment dels S.I. (INI/DOC – 006)**
  - Millora resultats observats A.R.
  - Focalitzat sobre Domini 12
- **Tractament de la gestió d'incidents en la seguretat de la informació (INI/PROC – 005)**
  - Focalitzat sobre Domini 13
- **Control de compliment dels procediments/normes i requeriments legals (INI/AUDIT – 001)**
  - Focalitzat sobre Objectiu de control 15.2 i 15.3

Evolució de l'impacte després de la implantació de les iniciatives

ACTIU		IMPACTE POTENCIAL (IP)					IP després Projectes				
		C	I	D	A	T	C	I	D	A	T
[S.1]	Servei de Correu Usuaris	6,80	5,25	8,00	3,90	5,10	**3,80**	**1,25**	**0,80**	1,70	**4,20**
[S.3]	Servei Intranet	6,00	6,00	6,00	4,50	2,45	**3,00**	**1,40**	**0,60**	1,80	2,00
[S.4]	Servei Web Marca [X]	5,10	5,25	5,00	2,00	3,00	**2,10**	**1,40**	**0,60**	1,80	2,80
[S.5]	Servei Web Marca [Y]	5,10	5,25	5,00	2,00	3,00	**2,10**	**1,40**	**0,60**	1,80	2,80
[S.6]	Servei Web Marca [Z]	5,10	5,25	5,00	2,00	3,00	**2,10**	**1,40**	**0,60**	1,80	2,80
[S.7]	Servei Web Promoció [2X]	5,10	5,25	5,00	2,00	3,00	**2,10**	**1,40**	**0,60**	1,80	2,80
[S.10]	Servei SKEP	1,75	4,50	5,95	1,05	1,25	1,50	0,75	**1,50**	1,00	1,10
[S.11]	Servei Intercanvi de Fitxers	1,50	0,75	3,40	1,00	0,60	1,10	0,75	0,20	1,00	0,60
[S.12]	Servei INFOLOG	2,50	3,60	5,00	1,75	1,25	2,20	1,40	**1,75**	1,25	1,25
[S.13]	Servei SGANL	1,75	3,50	6,00	0,75	1,25	0,75	2,10	**0,75**	0,75	1,25
[S.16]	Servei PRISMA	1,05	3,50	3,00	0,45	0,75	1,05	3,20	1,30	0,45	0,75
[S.17]	Servei ORALIMS	2,45	5,85	6,00	1,35	2,25	1,75	1,75	**1,90**	1,35	2,25
[S.18]	Servei CALOR	3,00	4,00	9,50	2,00	2,00	0,70	0,90	**2,10**	2,00	2,00
[S.20]	Servei FileServer ES	3,00	2,40	5,95	1,40	1,00	0,50	0,70	**0,20**	1,00	1,00
[S.21]	Servei FileServer PT	3,00	2,40	5,95	1,40	1,00	0,50	0,70	**0,20**	1,00	1,00

Evolució del Nivell de Compliment ISO



Canvis Organitzatius conseqüència del PDS

- La iniciativa "INI/ORG – 001" **implica canvis organitzatius:**

  - **Consolidació de les responsabilitats de S.I.**
  - **Consolidació del comitè de Seguretat/Salut**
  - Assignació de partides pressupostaries per l'àrea de S.I. Dintre dels "budgets" anuals.
  - **Nova metodologia de treball per evolucionar constantment la S.I.** A totes les àrees de l'organització
  - **Necessitats de recursos personals** per absorbir les noves tasques.

Resum Objectius assolits amb les iniciatives

Un cop finalitzada les fases prèvies corresponents a l'anàlisi de riscos i l'auditoria de compliment dels diferents capítols marcats des de la norma ISO, estem en disposició:

- Preparar **les iniciatives per evolucionar** l'estat actual de la S.I.
- **Decidir ràpidament i amb argumentació** quines tenen o no sentit.
- Establir un **seguiment per garantir l'evolució**
- Preparar una **visió complerta dels canvis** a implementar durant el període inicial d'aquest PDS

- **COMENÇAR EL TRACTAMENT DE LA S.I. COM UN PROCÉS CONSTANT DE MILLORA CONTINUA** amb disposició de recursos per tal de realitzar-la.

CONCLUSIONS del PDS

Per a l'organització; la realització d'aquest PDS, ha permès:

- **Canviar l'enfocament i el tractament** que es donava a la **Seguretat de la Informació** en totes les àrees de l'organització.
- **La realització d'un Anàlisi de Riscos complert**, on es presenta els **valors dels actius**, **les amenaces** a les quals estan exposats i **l'impacte potencial** que tindria la materialització de les mateixes.
- **La realització d'una auditoria de compliment de l'ISO/IEC 27002:2005** que els permet conèixer el nivell de compliment – e incompliment -.
- Dissenyar **un pla d'evolucions/iniciatives/projectes a implantar** durant la vida d'aquest PDS inicial, de cara a **arribar als objectius fitxats** des de la direcció de l'organització.

CONCLUSIONS del PDS

Per a l'estudiant de la UOC, encarregat de realitzar-ho, ha suposat:

- L'oportunitat de **preparar un PDS des del principi fins al final, realitzant totes les fases** marcades per tal de tenir els elements suficients a l'hora de poder decidir quins projectes s'han d'implementar en una organització i perquè.
- L'oportunitat de **realitzar un anàlisi de Riscos** sencer partir d'uns documents base ja que normalment a la vida laboral, es parteix de treballs previs realitzats per altres persones.
- Una **ampliació en els coneixements de la metodologia de MAGERIT.**
- Una **experiència sencera a nivell de Seguretat de la Informació** Que a permès **valorar la importància de tots els punts establerts a la normativa ISO.**
- **Confecció d'un llistat d'iniciatives** a implementar a nivell global durant un període de 4 anys per arribar als objectius definits des de la direcció de l'organització.


The End