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

Memòria Descriptiva

Taula de Continguts

1.- PRESENTACIÓ CAS D'US

1.1.- Presentació

Per la realització d'aquest projecte, hem seleccionat una multinacional a nivell europeu del sector de la gran distribució en el sector alimentari, i més concretament la seva divisió de refrigerats per la regió Ibérica. Aquesta divisió es dedica principalment a la fabricació i comercialització de iogurts i postres pel mercat espanyol i portuguès dintre de la gran distribució amb la incorporació d'un sistema de distribució per poder donar cobertura a la capil·laritat dels "petits comerciants" (tots els punts de comercialització que no es troben agrupats dintre d'un client de gran distribució alimentaria). A la seva vegada, existeix una tercera línia de treball enfocada a la fabricació i comercialització de la "marca blanca" (també anomenada MDD, Marca De Distribució) de les grans ensenyes del sector dintre d'aquest dos països.

De cara a poder parlar durant la realització d'aquest projecte d'aquesta divisió, anomenarem a partir d'ara aquesta divisió com **"UOC Postres S.A."**

Simplement per resumir de manera general les bandes d'actuació de l'empresa, podem afirmar clarament que la seva activitat esta focalitzada en:

- Fabricació de productes refrigerats de la marca "UOC Postres".
- Fabricació de productes refrigerats de MDD.
- Comercialització marca pròpia per a grans comptes.
- Comercialització marca pròpia per capil·laritat (petits clients).
- Comercialització MDD. (grans comptes)

Clarament podem observar que troben dues àrees diferenciades en la que es divideix la nostra empresa; d'una banda la part industrial, que s'encarrega de la producció; i d'altre, la part comercial que s'encarrega de la comercialització complerta (venda més distribució) del producte.

En aquest punt, a nivell de sistemes de la informació, simplement indicar que totes dues àrees treballen amb sistemes comuns i per tant interrelacionant la part industrial amb la part comercial. En els següents apartats podrem observar amb més detalls de quins sistemes estem parlant i con es produeix aquesta interrelació.

1.2.- DADES RELLEVANTS DE L'EMPRESA

En aquest apartat, indicarem algunes dades significatives referents a la nostra empresa que ens permetran aprofundir amb més detall en el cas d'us en el que ens trobem treballant:

Centres de treball: 1 fabrica a Espanya

2 Headquarters (ES+PT)

7 oficines comercials (ES+PT)

2 Centres de distribució ("CD", ES+PT)

*A nivell Europeu existeixen 7 fabriques per produir la gama complerta de productes que presenta el catàleg.

Treballadors a Espanya: 400 treballadors a la fàbrica

150 treballadors al centre de distribució

60 treballadors a les oficines centrals

40 treballadors a la força comercial

Treballadors a Portugal: 60 treballadors al centre de distribució

50 treballadors a les oficines centrals

32 treballadors a la força comercial

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

*Estem parlant del segon fabricant a nivell de quota de mercat en tots dos països. (El primer productor i la MDD acaparem gairebé el 88% del mercat).

Quota de mercat MDD (respecte MDD total): ES 89% / PT 52%

*Es tracta del primer fabricant de MDD als dos països.

Centres de Procés de dades (CPD): 1 CPD per tots dos països.

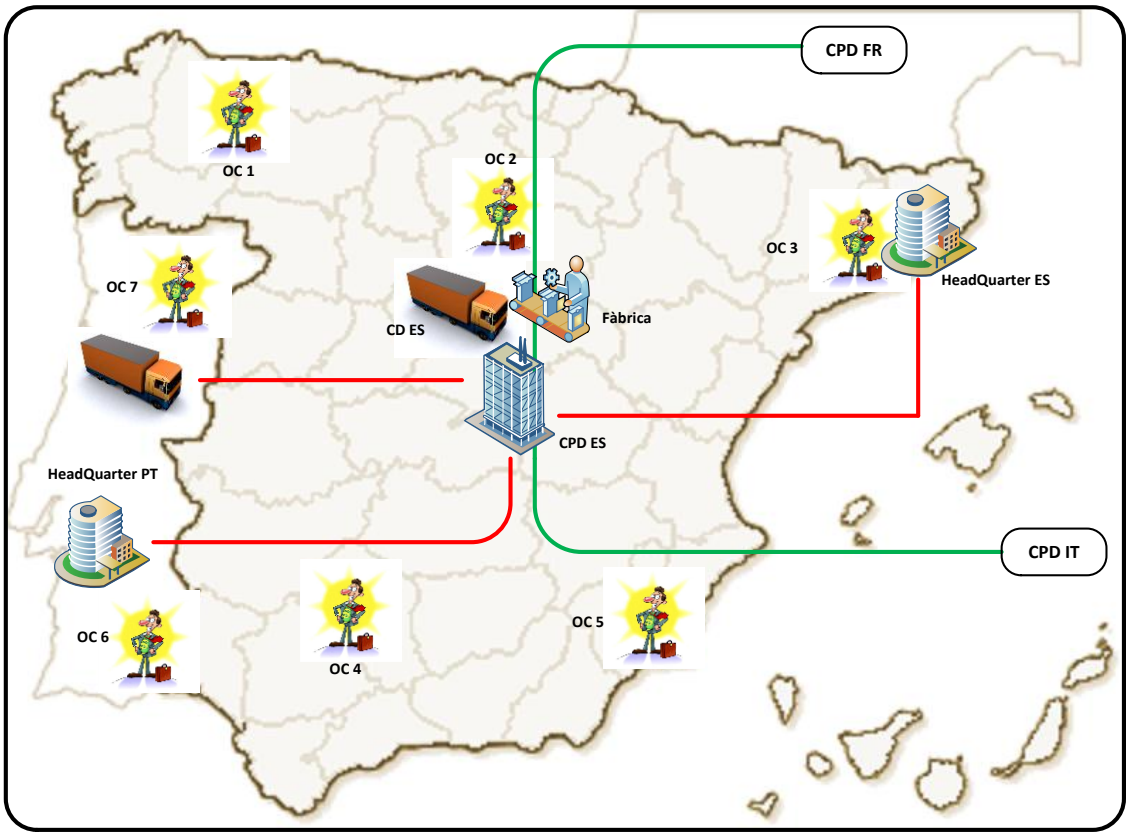
1.3.- DADES RELLEVANTS A NIVELL DELS SISTEMES DE INFORMACIÓ

1.3.1.- Esquema de la Xarxa

1.3.1.1.- Situació de les Seus de l'empresa

Al següent esquema podrem visualitzar gràficament com queda la connexió de totes les seus laborals que conformen l'estructura de la nostra empresa i com s'estableixen les connexions amb els CPD's ubicats a França e Itàlia, que donem servei sobre la nostre societat per la confecció d'aquest Pla Director.

En aquest esquema podem visualitzar la ubicació del Centre de procés de Dades per Espanya (CPD ES), les dues seus principals de la societat (HeadQuarter ES i HeadQuarter PT), la ubicació de la fàbrica de producció de la regió Ibérica (Fàbrica), la posició dels dos centres de distribució (CD ES i CD PT) com la ubicació de les set oficines comercials utilitzades per la xarxa de comercialització (OC "x").



***** No s'ha indicat cap tipus de connexió entre les Oficines Comercials (OC's) i el centre de procés de dades ja que com veurem en els apartats següents; les eines utilitzades per aquest equips de treball es trobem accessibles via Internet i per tant no necessiten una connexió directe contra el CPD.

La **Seu Central,** allotja en les seves instal·lacions el CPD ES, la fàbrica de producció, el centre de distribució per Espanya i l'oficina comercial per la regió centre.

1.3.1.2- Descripció connexions entre Seus Ibèriques

A nivell informàtic referent a la interconnexió dels diferents centres de treball, ens trobem davant d'un model clar de **xarxa en "disseny en estrella"** on trobem un CPD central que dona connexió a tots els centres de tots dos països, i esta interconnectat directament amb els CPD's de França (central europea de la societat) i el CPD de Itàlia (connexió directe contra el ERP del grup ubicat en Itàlia). Aquest CPD central s'encarrega de allotjar:

- Infraestructura sistemes de informació interns.
- Sortida a Internet.
- Connexió directe CPD FR i CPD IT.
- Equips de seguretat perimetrals (Firewall).
- Hosting dels diferents dominis web de la societat.
- Serveis interns considerats bàsics pels usuaris (correu, FileServer, etc.)

Dintre de les diferents seus que trobem, cal destacar que les agrupacions anteriorment comentades (fàbrica, Headquarters i oficines comercials) presenten tots ells les mateixes característiques a nivell de connexió i corresponen a:

Centre de Procés de Dades:	Línia Principal → Fibra Òptica 30 Mbps (dedicada).
	Línia Backup → Enllaç Radi 30 Mbps (dedicat).
	Routers Redundants.
Fabrica:	Línia Principal → Fibra Òptica 10 Mbps (dedicada).
	Línia Backup → ADSL 2 Mbps (dedicada).
	Routers redundant.
Headquarter:	Línia Principal → Fibra Òptica 5 Mbps (dedicada).
	Línia Backup → ADSL 2 Mbps (dedicada).
	Routers redundants.
Centre de Distribució:	Línia Principal → Fibra Òptica 5 Mbps (dedicada).
	Línia Backup → Enllaç Radi 5 Mbps (dedicat).
	Routers Redundants.
Connexió oficina comercial:	Línia Principal → ADSL 5 Mbps (40% garantit)
	Línia Backup → RDSI 512 Kbps dedicats
	Router NO-Redundat.

***Al tractar-se d'un disseny en estrella, totes les connexions són gestionades a nivell de la seu central que es on es troba ubicat el CPD (ES).**

1.3.1.3.- Descripció connexions amb CPD's Internacionals

Com hem pogut veure sobre l'esquema de seus que presenta l'organització en la Regió Ibèrica; el CPD utilitzat per donar servei tant a Espanya com a Portugal; es troba connectat directament al CPD de França, que realitza la funció de CPD central per tots els països d'Europa; i també es troba connectat amb el CPD de Itàlia que allotja a les seves instal·lacions l'ERP utilitzat per la multinacional a totes les seves divisions.

Cal destacar però en aquest punt, que aquesta connexió amb els CPD's Internacionals és **exclusiva** per la utilització de serveis que es troben allotjats a l'exterior i ofereixen aquest servei per la resta de països i divisions (es tracta d'un tema de centralització per economia d'escala).

Un cop aclarit quin es l'ús d'aquestes connexions internacionals, indicarem quina es la infraestructura utilitzada per aquestes connexions:

Connexió CPD FR: 4 línies dedicades 100% garantides de 2 Mbps (Fibra Òptica).

2 canals principals i 2 canals com a Backup.

Routers Redundants.

Connexió CPD IT: 2 línies dedicades de 2 Mbps (Fibra Òptica 100% Garantides).

1 canal principal i 1 canal com a Backup.

Routers Redundants.

1.3.2.- Sistemes de Informació

1.3.2.1.- Esquema Principal dels Sistemes de Informació

Dintre dels sistemes de la informació utilitzats per aquesta empresa podem trobar una primera classificació inicial que es correspon a la separació dels serveis/sistemes bàsics que el grup a decidit que tots els usuaris hauran d'utilitzar i després trobarem tota la resta de sistemes que poden donar cobertura a les diferents necessitats dels diferents departaments interns que trobem dintre de la societat. Per tant, realitzarem una primera presentació –a alt nivell- dels diferents sistemes utilitzats a la societat de cara a tenir unes primeres dades de utilització, funcionalitat i situació dels diferents sistemes respecte a la societat i la seva funcionalitat i posteriorment donarem els detalls de com es troben dissenyats aquests sistemes.

1.3.2.1.1.- Sistemes bàsics/estàndards (comuns a tots els usuaris)

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

- Sistema d'Enterprise Resource Planning *(ERP - SAP)*

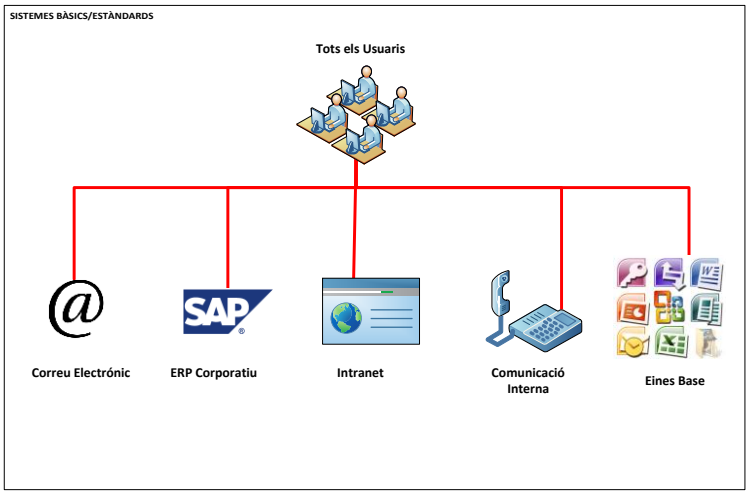
* Donant cobertura als mòduls:

- Comptabilitat
- Facturació
- Control de gestió
- Vendes + Business Intelligence
- Facturació logística
- Recursos Humans

- 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.)



1.3.2.1.2.- Sistemes concrets de l'organització

Sistema de gestió de magatzems (INFOLOG + SGANL)

Aquest sistemes son utilitzats en el departament de logística de l'organització i permeten principalment la gestió del magatzem de producte terminat (INFOLOG) i dels magatzems de matèria prima (SGANL). Dintre d'aquest sistemes es troba implementada la

lògica de negoci establerta per la gestió d'aquest tipus de magatzems i que sense entra en detall ha de complir d'una banda la política de treball de "just in time" que resumidament estableix els criteris pertinents per tal de produir sota demanda de cara a evitar sobre estocs de producció o la immobilització de capital amb estocs massa grans. A la seva vegada s'ha d'evitar arribar a situacions de ruptura on no hi hagi matèria prima o producte per servir al mercat. D'aquesta primera definició veiem clarament que aquest sistema treballa relacionat molt estretament amb els sistemes de planificació de la producció i venda de l'organització. A nivell de funcionament, podem ressaltar que es tracten de sistemes que mitjançant la radiofreqüència i terminals utilitzats en els magatzems permeten treballar en una situació real en tot moment.

Presenta con elements destacats tota la infraestructura necessària per implementar la radiofreqüència sobre els magatzems i tots els tipus de terminals que els empleats podem utilitzar per interactuar amb el sistema.

Sistema de gestió de manteniments i serveis tècnics (PRISMA)

Es tracta del sistema de gestió establert pel departament tècnic industrial de cara a gestionar tot el manteniment i reparacions de tota la maquinaria que gestionen sobre les fabriques del grup. De cara a consolidar un valor inferior de estoc en els recanvis de valor elevat, aquesta eina treballa amb una base de dades comuna per a totes les fàbriques de cara a gestiona un inventari conjunt d'aquest tipus de recanvis (normalment elements de valor superior a 30.000€).

A part del mòdul de gestió de l'inventari, presenta el mòdul de manteniment preventiu i proactiu i la gestió d'actuacions de l'equip tècnic.

Sistema de planificació de la producció (FUTURMASTER)

Sistema de planificació a mig (de 2 a 4 setmanes vista) i llarg termini (de 5 a 12 setmanes vista) per tal de poder gestionar les previsions de venda i poder evitar les situacions de ruptura o sobre producció abans comentades. Degut a que la producció del catàleg complert de productes es troba distribuïda entre totes les fabriques d'Europa, aquest sistema es troba centralitzat en el CPD de França i tots els usuaris accedeixen mitjançant una connexió CITRIX. Per tal de complir la seva funcionalitat presenta diferents interfícies de comunicació amb diferents sistemes de l'organització com podem ser la gestió de magatzems o la pròpia eina inclosa en l'ERP de la companyia de simulació de vendes.

Sistema de planificació de necessitats (SKEP)

Es tracta del sistema local utilitzat a les fabriques que s'encarrega de planificar la fabricació de la setmana actual en funció de les necessitats dels diferents mercats, la disponibilitats de materials o la pròpia millora de la productivitat causant el menor impacte possible sobre el procés de fabricació agrupant fabricacions i evitant parades innecessàries. Es troba interrelacionat amb l'eina de planificació a llarg termini i les eines de gestió de magatzem, com la gestió de comandes realitzades des de l'ERP de la companyia.

Sistema de gestió de la qualitat (ORALIMS)

Sistema utilitzat pel departament de qualitat per gestionar la qualitat del producte en totes les seves fases de producció. Es troba relacionat amb el sistema de gestió de magatzems de producte terminat per tal de garantir la traçabilitat dels productes. Físicament presenta interfícies amb diferents eines de laboratori per tal de procedir a la adquisició de totes les dades necessàries per tal de garantir la qualitat.

Sistema gestió punt de Venda (CALOR)

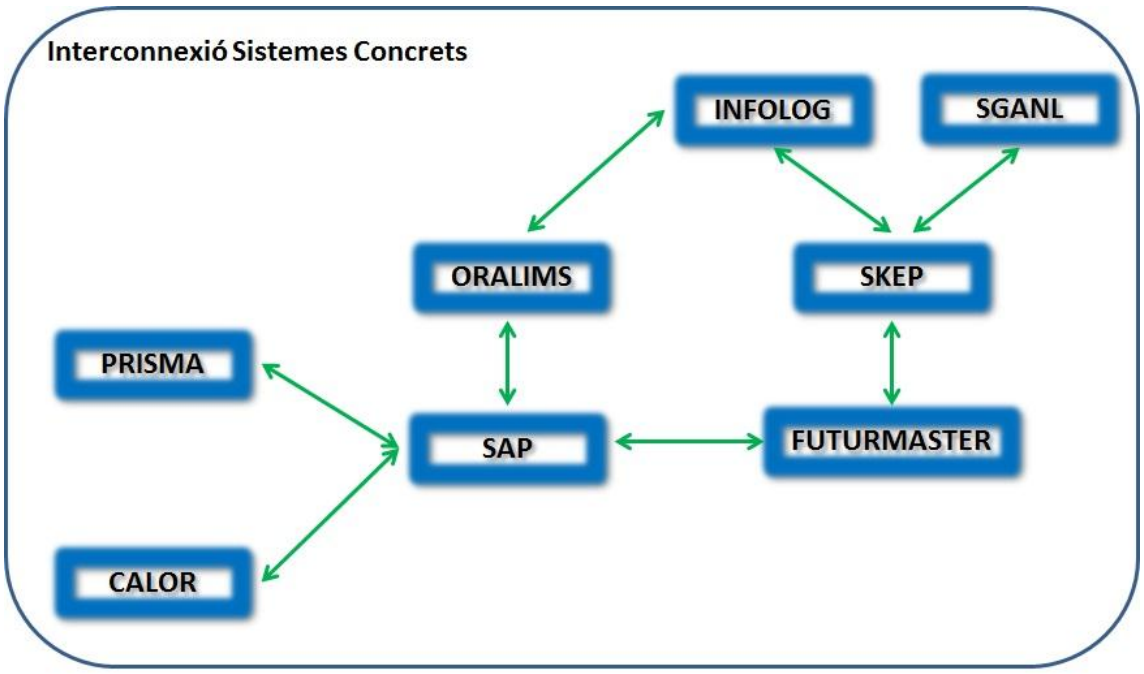
Es tracta del sistema que s'encarrega de gestionar totes les comandes que no provenen pel canal de gran distribució, es a dir, les comandes de la capil·laritat anteriorment comentada. Aquesta plataforma presenta diferents mètodes d'entrada o recepció de les comandes com poden ser:

- Sistema automatitzat de recepció de fitxers d'e-mail.

- Gestió telefònica.

- Gestió agrupada per majorista.

- Presa manual mitjançant terminals mòbils des de l'equip de força de ventes.



* A part d'aquest sistemes, també podem trobar sistemes tancats que trobem al mercat per donar suport a les diferents àrees de treball de la empresa però que no presenten cap particularitat especial ja que es tracten de llicències d'us ja siguin internament, com podríem ser les instal·lacions locals o en xarxa de sistemes concrets. Externament també trobarem les llicències d'us d'eines de tercers que solament requereixen una connexió a internet.

1.3.2.2.- Detall Tècnic dels Sistemes de Informació

Una vegada hem conegut les funcionalitats o funció dels sistemes de la informació de l'empresa; entrarem a realitzar una primera aproximació per conèixer amb més detall tècnic com es trobem implantades aquestes solucions i tenir una base de cara als posteriors apartats d'aquest document on s'estudiarà la seguretat d'aquestes configuracions per als sistemes comentats, els propis actius que conformin aquest sistemes de la informació o poder decidir quines amenaces poden afectar-los.

Cal destacar que no entrarem en el detall de com es realitzem les copies de seguretat de cada sistema o el propi manteniment que tenen contractat a nivell físic (apart que es podria dedicar tot un apartat al respecte) ja que assumint que en cada cas es troba en una situació optima, ja que en el moment d'implantar cada sistema es va realitzar a propi del sistema un anàlisi de riscos per tal de evitar males configuracions inicials. Tot i això si en qualsevol dels sistemes detectéssim una deficiència en algun d'aquest punt; ho indicaríem en aquest document per tal de poder tenir-ho en compte pel anàlisi de riscos que realitzarem en la confecció d'aquest PDS.

Per tant en aquest apartat, veurem sistema per sistema alguns detalls significatius de cadascun d'ells:

Sistema de Correu

El sistema de correu utilitzat per l'organització és Microsoft Exchange en la seva versió 2003. Com a client correu pels usuaris s'està utilitzant la solució estàndard de Microsoft anomenada Outlook en la seva versió 2010.

En relació a la seva infraestructura, podem comentar que existeixen un servidor físic que realitza la funció de Servidor Principal de Correu i que es troba dedicat en exclusiva a aquesta tasca i després trobem 2 servidors més, també físics, ubicats als HeadQuarters de cada país, que realitzem la funció de "Back-end" en la infraestructura necessària per la solució de correu. Aquest dos servidors no son dedicats, i presenten també la funció de FileServer, Active Directory i software local per cadascun de les dues seus on es trobem instal·lats.

A la seva vegada, existeix un darrer servidor a tenir en consideració en aquesta solució, que també es troba ubicat dintre del CPD de la societat, que realitza la funció de "Front-end" per tal de poder publicar el correu via internet (OWA – Outlook Web Acces) i permetre l'accés tant des de Internet com dels propis dispositius mòbils.

Per últim cal destacar que la solució utilitzada per el filtratge tant del correu d'entrada com de sortida tant a nivell de Spam com de virus consta de 2 appliance hardware (Principal i Backup) que es troben ubicats al CPD i s'encarreguen de revisar tot el correu de l'organització a nivell ibèric. En Resum, trobem:

- Servidor Físic dedicat *"ESWK3MAD02"* ubicat al CPD.
- Servidor Físic dedicat *"SRVMAD13"* ubicat al CPD.
- 2 x IronPort físic ubicat al CPD.
- 2 x Servidors Físic *"ESWK3COR902"* i *"PTWK3CAR902"* ubicats als HQ's.

Sistema ERP

Queda fora de l'abast de la confecció d'aquest PDS i simplement hem de controlar les línies de comunicació (i els seus routers) per tal de poder proveir la connexió a tots els usuaris contra el CPD Itàlia.

A nivell de instal·lació es tracta d'un sistema Client – Servidor, que presenta una instal·lació local sobre la màquina de l'usuari per tal de poder utilitzar el sistema.

Sistema de Comunicació Interna

Per tal de poder utilitzar el sistema de comunicació interna pels usuaris del proveïdor Microsoft anomenat Office Communicator 2007, existeixen dos servidors dedicats per tal de poder gestionar d'una banda tota la part de comunicació VoIP, ja que mitjançant els equips dels usuaris tenen la possibilitat de parlar amb els seus companys de tota l'organització a nivell europeu, i com a segona opció es manté el client de missatgeria instantània que l'eina incorpora per tal de poder proveir aquest servei a tots els usuaris. Aquest sistema és una solució Client – Servidor on els usuaris presenten una instal·lació local que els permet utilitzar el sistema.

Per tant trobem:

- 2 servidors físics dedicats "ESWK3MAD905" i "ESWK3MAD906" ubicats al CPD.

Cal destacar però, que tot i ser 2 servidors pel mateix sistema, no estan configurats com Backup l'un de l'altre ja que realitzem tasques completament diferents.

Intranet Corporativa

L' intranet corporativa esta dissenyada per una empresa externa que s'encarrega de donar el servei de manteniment com de realitzar les corresponents evolucions o millores però es troba allotjada a la infraestructura interna que es té a l'organització per donar cobertura a totes les solucions webs de les diferents divisions que hi ha dintre de l'organització. Principalment existeixen d'altres pàgines webs en relació a marques, productes, promocions o campanyes de comunicació amb els clients.

En aquest cas, trobem que el sistema presenta d'una banda la solució dissenyada per la Intranet, i utilitza una Base de Dades (Microsoft SQL Server 2008) per emmagatzemar tota la informació. Donat que existeix una infraestructura dedicada per tota la part de servei web, existeix una solució de Virtualització complerta, mitjançant la utilització d'un chasis Blade per allotjar 3 servidors físics amb una cabina de disc autogestionada per tal de garantir la major disponibilitat d'aquest servei. Amb aquesta infraestructura breument comentada, s'aconsegueix independència física de les dades que es trobem ubicades dintre de la pròpia cabina que s'autogestiona per donar servei constant amb independència dels servidors que a l'hora es trobem virtualitzats sobre els tres servidors físics anteriorment comentats per tal de poder evitar al màxim possible les fallades físiques del mateixos. Aquesta infraestructura ha estat disposada així, ja que bàsicament en el moment de "internalitzar" totes les pàgines web

de l'organització sobre la infraestructura, es va realitzar l'estudi exclusiu d'aquest apartat per tal de reduir al màxim possible (amb un preu raonable) les possible amenaces relacionades amb la infraestructura interna.

Per tant en el nostre CPD en aquest cas, trobem:

- Chasis Blade amb:
    - 3 servidors físics "SRVMAD21", "SRVMAD22" i "SRVMAD23".
    - 1 cabina de discos

Eines Base

Aquest apartat, l'hem utilitzat a l'apartat anterior per agrupar tota la sèrie d'aplicacions utilitzades pels usuaris i que solem ser eines propietàries instal·lades sobre els propis equips dels usuaris i per tant només destacarem que existeix un servidor intern ubicat al nostre CPD per tal de realitzar la distribució i l'inventari de llicencies d'aquestes eines.

Aquest servidor és físic i esta dedicat exclusivament per la tasca de distribució, inventari i actualització d'aquest tipus de sistemes.

Eines Base pels SI

Abans de passar a comentar els detalls tècnics de les eines concretes utilitzades per l'organització, ens agradaria incloure dos serveis utilitzats pel departament de Sistemes de La informació a nivell de seguretat de la xarxa i que presenten també dos servidors físics dedicats per tal de poder realitzar les tasques pertinents a les que estan encomanats. En aquest cas estem parlant del servei d'antivirus per l'organització i el servei de Firewall per garantir la seguretat de la xarxa.

En el cas de servei d'antivirus trobem un servidor físic que s'encarrega de la distribució d'actualitzacions a tots els clients dintre de la xarxa corporativa.

A nivell de Firewall, s'ha optat per una solució software "Microsoft ISA Server 2006" que s'encarrega de realitzar les tasques de publicació, enrutament i securitzar els accessos des de l'exterior cap a la xarxa interna. En aquest cas s'ha optat pel disseny d'una configuració d'una xarxa amb tres potes on es controla el tràfic entre la xarxa externa, la xarxa interna i la zona desmilitaritzada.

A nivell del CPD trobem:

- Servidor físic repositori antivirus "SRVMAD03".

- Servidor físic Firewall "SRVMAD12".

FUTURMASTER

Aquest sistema es troba ubicat al CDP de FR ja que ha de coordinar les previsions de tots els països dels diferents mercats Europeus i per tant es troba fora de l'abast d'aquest PDS ja que es trobarà garantit ple PDS corresponent de França. A nivell de connexió simplement comentar que els usuaris podem accedir als sistemes mitjançant el client CITRIX que tenen instal·lat sobre els seus ordinadors sempre i quan es trobin treballant en la xarxa corporativa.

SKEP

Aquesta aplicació es troba instal·lada a nivell central en les instal·lacions del CPD ES sobre el servidor d'aplicacions "SRVMAD05" que es un servidor físic on s'instal·len varies aplicacions utilitzades a varies seus de l'organització. En aquest cas, aquest sistema presenta les dades guardades sobre la pròpia instal·lació (no utilitza cap base dades externa) i es gestionada mitjançant els seus propis fitxers interns.

La connexió dels usuaris cap al servidor es realitza mitjançant el aplicatiu client instal·lat a l'equip de l'usuari.

La comunicació d'aquest sistema, amb els sistemes de Futurmaster, Infolog i Sganl es realitza mitjançant l'intercanvi de fitxers que esta configurat sobre algunes carpetes d'aquest propi servidor.

Es realitza una copia diària de seguretat (a les 00:00h) tant dels fitxers d'informació del sistema com de les carpetes d'intercanvi amb la resta de sistemes.

INFOLOG

Aquest sistema esta dissenyat sobre la plataforma de IBM anomenada AS400 i es troba centralitza en la màquina d'AS400 ("ESAS400") que es troba instal·lada al CPD ES. A la seva vegada, existeix un segon equip d'AS400 configurat com a replica d'aquest primer, i que es troba configurat amb duplicació sincronitzada del primer sistema per tal de garantir el servei en cas de problema físic sobre el primer servidor.

Aquesta configuració, prové d'un segon CPD que s'havia utilitzat en el passat quan dintre de la plataforma d'AS400 trobàvem tant el control de la producció a nivell de fabricació com el propi ERP de l'organització però en el moment de la migració d'aquest sistemes cap a SAP es va decidir tancar aquest segon CPD i mantindré aquesta segona màquina d'AS400 com a replica de la principal. Per tal de evitar problemes dintre del CPD (i per temes de disponibilitat d'espai) es va decidir ubicar aquesta segona màquina dintre de la sala de servidors/comunicacions de la fàbrica ja que es troba a uns 600 metres de distancia del CPD ES amb una connexió directa per fibra òptica que permet realitzar aquest tipus de sincronització.

A nivell de backup, es realitzem copies diàries de les dades del sistema i copia setmanal de les configuracions del sistema que son emmagatzemades a la caixa forta que existeix per aquesta finalitat a les instal·lacions on es troba CPD.

Cal destacar que aquest programa te comunicació en tots dos sentits en temps real tant amb els terminals de mà utilitzats per la gestió de producte terminat com la pròpia preparació de les comandes que provenen dels clients.

A nivell d'usuari s'utilitza una aplicació client (Client Access v.5.03) per tal de poder connectar amb el servidor per la seva utilització.

SGANL

Aquest sistema es troba instal·lat sobre el servidor d'aplicacions "SRVMAD05" però en aquest cas presenta tota la seva estructura de dades sobre la base de dades de Microsoft SQL Server 2008 que es troba instal·lada sobre el servidor "SRVMAD06".

Es tracta d'una aplicació client – servidor, que permet tant als clients fixos com els propis terminals de ma utilitzats al magatzem connectar directament amb el sistema per tal de poder gestionar les matèries primes.

SAP

Com ja hem indicat anteriorment, la infraestructura utilitzada per aquest sistema es troba ubicada al CPD Itàlia i per tant queda fora del abast d'aquest pla director.

La connexió dels usuaris es realitza mitjançant l'aplicació client instal·lada sobre els equips dels propis usuaris.

PRISMA

Aquest sistema es troba instal·lat sobre el servidor d'aplicacions "SRVMAD05" però en aquest cas presenta tota la seva estructura de dades sobre la base de dades de Microsoft SQL Server 2008 que es troba instal·lada sobre el servidor "SRVMAD06".

Els usuaris del sistema presentem la part client instal·lada sobre els seus ordinadors per tal de poder connectar amb el sistema.

ORALIMS

Aquest sistema es troba instal·lat sobre el servidor d'aplicacions "SRVMAD05" però en aquest cas presenta tota la seva estructura de dades sobre la base de dades de Microsoft SQL Server 2008 que es troba instal·lada sobre el servidor "SRVMAD06".

Els usuaris del sistema presentem la part client instal·lada sobre els seus ordinadors per tal de poder connectar amb el sistema. En aquest cas, a part dels propis usuaris del sistema cal destacar que es realitza l'adquisició de dades que provenen dels instruments de control i mesura de la qualitat establerts durant tot el procés de fabricació i que reportem la informació al sistema mitjançant una carpeta d'intercanvi de la informació que es troba sobre el mateix servidor.

En alguns casos concrets on la instrumentació no ha permès la connexió directe amb el sistema s'han preparat equips intermedis per tal de realitzar aquestes adquisicions. Aquest equips intermedis els deixarem fora d'aquest PDS principalment perquè estan considerats com

instrumentació industrial (al igual que qualsevol maquinaria de producció) i segon perquè son simples equips utilitzats per donar la funcionalitat de connexió a la xarxa als instruments que no podem realitzar-lo directament.

CALOR

Aquest sistema té assignat un servidor físic dedicat ("SRVMAD08") tot i que presenta també les dades emmagatzemades sobre el propi servidor corporatiu de Bases de Dades de Sql Server 2008 ("SRVMAD06"). En aquest cas, dintre d'aquest servidor dedicat per la aplicació, trobem diferents mòduls encarregats de rebre en cada cas les diferents vies d'accés al sistema per a la informació, ja sigui des de el terminals portàtils que porten els propis venedors com des de el propi client per ordinador que existeix pel departament de suport a vendes. A la seva vegada aquest servidor s'encarrega de reportar la informació cap a l'ERP de la companyia i rebre la informació referent a vendes que s'encarregarà de servir als propis usuaris de la part comercial. S'utilitza en aquest punt, com a servidor de distribució de la informació comercial per als equips de vendes.

En aquest cas i donat les necessitats establertes per la direcció comercial, es realitzem quatre copies de seguretat diàries (cada 6h.) per tal de poder mitigar els riscos en cas de problema amb les dades amb les que treballa el sistema ja que la recepció de comandes esta oberta durant les 24 h. (en especial al sistema automatitzat per als grans clients).

A la seva vegada el propi servidor presenta una instal·lació prepara de SQL Server 2008 per tal de poder treballar de forma autònoma en cas necessari si el servidor corporatiu no estigues accessible per qualsevol circumstancia.

1.4.- ESTAT ACTUAL DE LA SEGURETAT DELS SISTEMES DE INFORMACIÓ

1.4.1.- Presentació Situació Actual

A nivell de la seguretat dels sistemes de informació, el primer que ens agradaria destacar, es que tot i trobar presents algunes mesures i criteris de seguretat sobre els sistemes de informació (i tot el relacionat amb els sistemes); **mai** s'ha realitzat un pla de seguretat de la informació i per tant aquestes mesures han sigut establertes sense el corresponent estudi previ o complert per analitzar la seva necessitat i justificació. Degut a aquest factor, podem avançar que trobarem mesures inexistents, mesures sobredimensionades, mesures correctes, desconeixement de les possible amenaces a les que els sistemes es troben exposats, desconeixement dels riscos que aquestes amenaces comporten pel negoci o la pròpia quantificació econòmica de l'impacte d'ocórrer les diferents amenaces.

A nivell de la normativa aplicada o les possibles bones pràctiques definides o criteris interns de gestió de la seguretat de la informació, la situació no es molt millor ja que ens trobem amb una organització on mai s'ha donat molta importància a la seguretat dels sistemes de la informació com a tal, sinó que sempre s'ha tractat de manera puntual o en punts concrets degut a la legalitat vigent a complir en cada moment, com seria el cas de la LOPD. Per tant, observem que no existeix cap normativa de seguretat, pla de contingència o fins i tot trobem que no existeix un anàlisis de riscos per tal de conèixer els riscos als quals es trobem exposats per estar en aquesta situació.

En aquesta situació, podem realitzar una primera afirmació deguda principalment a la situació actual i es que podem considerar que els sistemes de informació es troben en una situació clara d'inseguretat principalment pel desconeixement de la situació actual, les amenaces a les quals es troba exposat i fins i tot el desconeixement del impacte que tindria sobre el negoci aquests riscos al quals es trobem exposats. Ens agradaria remarcar en aquest punt, que fent aquesta informació, ja que tot i existir mesures concretes de seguretat implementades, considerem que sense tenir clar la situació ni la realització d'un anàlisi de riscos es completament impossible poder afirmar que estem davant d'un bon nivell de seguretat. Considerem que la qualitat de la seguretat i el seu nivell queda demostrat mitjançant aquest anàlisi de riscos que ens permetrà afirmar la qualitat de la seguretat. Ens podríem trobar davant d'una organització o s'haguessin implementat totes les mesures de seguretat necessàries però sense l'anàlisi de riscos no podríem afirmar que cobreixen totes les amenaces possibles, o quin es el risc residual existent que l'organització assumiria o fins i tot seria difícil plantejar un mètode de millora continua ja que esta basat en la anàlisi de la situació actual per arribar a una situació millor i que continuarà cíclicament evolucionant constantment

Donada aquesta situació, podem afirmar en aquest moment inicial, que la situació actual de la seguretat tot i presentar certes mesures establertes per mitigar certes amenaces, hem de classificar-la com una **situació precària** o un **nivell baix de seguretat** en els sistemes de la informació, degut fonamentalment a dos factors molt importants com son el desconeixement de la situació actual en la que es troba l'empresa, en termes de seguretat, i la impossibilitat que suposa aquesta falta de coneixement per tal d'implementar un mètode de millora continua sobre la seguretat de la informació.

Per tant, podem afirmar, que la necessitat primària en aquest punt per aquesta organització serà la implementació d'un pla director sobre la seguretat dels sistemes de informació.

1.4.2.- Descripció mesures de Seguretat Implantades

Durant la pròpia descripció dels sistemes de la informació presents a l'organització hem anat nombrant o comentant diverses mesures de seguretat implantades tant els propis sistemes com el la pròpia infraestructura, tant de comunicació com de servidors, i per tant aprofitarem aquest apartat per tal de parlar més amb detall de les mesures de seguretat física i lògica que trobem actualment instal·lades a la companyia i les seves instal·lacions que tenen relació amb els propis sistemes de la informació.

Per tant començarem parlant de la seguretat física que podem trobar sobre el propi CPD, on podem veure clarament que existeix la protecció contra incendis mitjançant procediments i normatives relacionades entorn al material que pot entrar en les instal·lacions i els medis de detecció per tal de mitigar-los en cas de produir-se. El control sobre aquesta àrea (com a la resta d'ubicacions de l'organització on hi ha infraestructura relacionada amb el departament de sistemes de la informació de l'organització) es troba restringit i controlat pel personal autoritzat. En aquest sentit també podem indicar que es realitza un control exhaustiu tant pel personal tècnic extern que pot haver de treballar sobre les instal·lacions com sobre els suports on la informació es troba emmagatzemada ja sigui de forma principal com en els corresponents Backups anteriorment comentats.

A nivell de les comunicacions hem pogut observar que existeixen acords de servei e integritat amb els propis proveïdors i donat que es realitza majoritàriament un ús de línies dedicades no s'utilitza cap sistema de encriptació o xifrat a nivell intern sobre les comunicacions però es restringeix l'accés a la xarxa corporativa solament als usuaris de l'organització. Algunes seus presenten una "connexió de cortesia" per poder oferir connexió a internet als possibles visitants externs a la companyia i esta garantida la separació física d'aquestes dues xarxes al tractar-se de solucions locals a les seus.

A nivell de instal·lacions podem comentar que trobem infraestructures redundants tant a nivell de cablejat com de distribuïdors de xarxa (switches) principalment dintre de la infraestructura del CPD com de la pròpia infraestructura que incorporem els sistemes de gestió de magatzems utilitzats amb la utilització de punts d'accessos repartits per tot el magatzem i que han de donar servei les 24h. Del dia. En l'apartat del la gestió de magatzems es va realitzar l'anàlisi de riscos en el moment de la implantació de la solució i donat a l'impacte que suposava la materialització de qualsevol amenaça sobre la infraestructura necessària, es va poder adoptar la redundància de gairebé tota la infraestructura utilitzada. Tot i això quan entrem més en detall en aquest punt, es possible que trobem algun punt on es podria realitzar algun retoc ja que des de que es va plantejar inicialment no s'ha verificat més aquesta seguretat i es possible que sigui necessari influir procediments de revisió i gestió.

A nivell dels sistemes simplement indicar que a nivell procedimental esta estipulat que cada cop que s'incorpora un nou servidor sobre l'organització s'ha de crear un procediment complert de recuperació des de cero per tal de garantir la continuïtat del sistema. En aquest document s'indica clarament d'on agafar la versió dels sistema utilitzat, com configurar-la i per últim com incorporar les dades relatives a l'organització des de l'últim cop que es va realitzar la copia de seguretat o com realitzar la connexió amb el sistema on es trobem emmagatzemats les dades. Cal destacar però que s'han detectat casos on la revisió d'aquest documents no s'ha realitzat i presenten certs problemes a l'hora de recuperar els sistemes per modificacions que s'han realitzat durant la vida del sistema. Cal destacar també en aquest punt, que tots els sistemes de la informació han sigut dissenyats per proveïdors externs que presenten contractes vigents per tal de realitzar el manteniment de les seves solucions com garantir les modificacions en cas necessàries. Podem destacar també l'existència de contractes de confidencialitat amb els proveïdors, principalment a nivell de la informació, ja que en alguns casos pot ser de vital importància respecte de la pròpia competència que resulta que també es client del propi proveïdor.

A nivell de la informació que es considera confidencial o d'accés restringit en l'organització podem comentar que l'única mesura observada de control es la gestió d'accessos per aquest informació però no hem detectat cap mesura de control per evitar la copia o duplicació de la mateixa.

A nivell dels equips d'usuari, existeixen mesures de protecció contra la utilització de codi perillós (virus, espies, etc.) com la gestió dels privilegis pels usuaris per evitar manipulacions en les configuracions base dels equips. Cal destacar en aquest punt que els equips que surten fora de la xarxa corporativa però necessiten accedir a sistemes solament accessibles des de la xarxa corporativa presenten una solució d'accés VPN amb verificació d'identitat) per tal de poder accedir als sistemes.

Com últim punt d'aquest apartat ens agradaria incorporar un comentari a nivell de les mesures de seguretat observades ja que hem detectat que no existeix cap mesura per evitar els propis atacs interns que pot sofrir els propis sistemes de la informació. Pel que hem pogut observar, existeixen algunes mesures de cara a garantir la seguretat respecte a l'exterior però a nivell intern no hem detectat cap. Caldria estimar si son o no necessàries dintre de l'organització.

1.5.- MOTIVACIÓ PER LA CREACIÓ D'AQUEST PLA DIRECTOR

1.5.1.- Motivació del PDS

La confecció d'aquest pla director serà la base del procés de millora contínua en matèria de seguretat per la societat, permetent a l'organització conèixer l'estat de la mateixa i plantejar les accions necessàries per minimitzar el impacte dels riscos potencials als quals es troba esposada.

Gracies a la confecció d'aquest pla, podrem veure definir clarament quina es la documentació normativa sobre les millors pràctiques en seguretat de la informació, podrem conèixer en tot moment quina es la situació actual en la que l'empresa es troba i els objectius futurs per tal de millorar aquesta situació.

De cara a poder complir aquest objectius:

- Identificarem i valorarem els actius corporatius com a punt de partida mitjançant el corresponent anàlisi de riscos.
- Avaluarem les amenaces i les classificarem.
- Avaluarem el nivell de compliment de la ISO / IEC 27002:2005 en l'organització (tot i no ser obligatòria per no tractar-se d'una empresa pública, es un clar referent per les empreses privades).

Aquest estudi complert mitjançant aquest pla director a implementar ens permetrà:

- Preparar propostes de projectes de cara a aconseguir una adequada gestió de la seguretat i millorar constantment la situació actual.
- Obtenir uns resultats clars que ens permetin presentar-los fàcilment i arribar a la comprensió dels mateixos per part de la pròpia direcció que sol validar les inversions dels projectes futurs.

1.5.2.- Abast del PDS

Donada la envergadura de l'empresa, i la dispersió que presenten els diferents sistemes de la informació entre els diferents centres de procés de dades; cal destacar que aquest Pla Director de la seguretat de la informació estarà enfocat al territori ibèric de la divisió ja que els sistemes que son proveïts des de els centres de procés de dades Internacionals estaran inclosos dintre dels corresponents plans directors dissenyats en els seus països on es troben ubicats. El proveïdor de l'altre país on es troben ubicats els sistemes, seran els responsables d'incloure sobre els seus plans directors aquests sistemes i garantir la seva seguretat. Per a nosaltres, seran tractats com a serveis extern on només tindrem la responsabilitat de garantir la connexió des de la nostra banda.

Per tant, en relació als serveis que provenen des de els CPD's internacionals, l'única part que haurà d'estar contemplada en el nostre PDS, serà la connexió amb els CPD's Internacionals a nivell de línies de comunicació i tota la infraestructura necessària per establir aquesta connexió que estigui ubicada al CPD ubicat a Espanya.

Un cop aclarit l'apartat Internacional, podem concretar amb més detall que la confecció d'aquest pla director estarà enfocada a donar cobertura a:

- 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.**
- Infraestructura complerta dels diferents sistemes de la informació.
- Connexió i provisió de comunicació amb els sistemes externs.
- **Serveis relacionats amb els sistemes de la informació proveïts des de el CPD ES cap a totes les seus de la Regió Ibèrica.**

A nivell departamental, veiem que aquest abast comentat tindrà impacte principalment sobre els departaments de logística, oficina tècnica, qualitat i comercial (i el propi departament de sistemes de la informació) ja que son els que presenten sistemes concrets per la realització de les seves tasques però no oblidarem que totes les eines bàsiques de tots els usuaris també estaran cobertes per aquest PDS, i per tant estaran inclosos dintre d'aquest abast amb menor importància.

Resum ABAST

Veiem que l'abast d'aquest PDS estarà focalitzat sobre la Regió Ibèrica i els sistemes de la informació que estan establerts dintre d'aquest perímetre d'actuació, i que es proveeixen com a serveis (i estaran classificats com actius del tipus Servei) per a tots els usuaris de l'organització.

Dintre d'aquest abast, realitzarem la valoració complerta de tots els actius implicats com hem indicat però **ens focalitzarem sobre els serveis oferts als usuaris que estaran focalitzats en:**

- **Serveis comuns als usuaris.**
- **Serveis específics anteriorment comentats.**

2.- PRESENTACIÓ DEL PLA DIRECTOR

El Pla Director de Seguretat (d'ara endavant PDS) constitueix el full de ruta que ha de seguir la nostra organització per gestionar d'una forma adequada la seguretat de tota la nostra informació i sistemes de la informació, permetent d'una banda conèixer clarament l'estat en el que ens trobem en tot moment (i a que ens exposem), i d'altre poder decidir clarament i amb arguments en quines línies s'ha d'actuar de cara a millorar la nostre seguretat. Gracies a aquestes dues afirmacions contundents dels objectius primordials d'aquest PDS, podem deduir clarament que el pla esta enfocat a introduir el model de millora continua, que com ja coneixem d'altres àrees de l'organització (en cas contrari, es pot llegir una petita aproximació al glossari d'aquest document a l'entrada corresponent al "cicle de Deming", també conegut com cicle o "model PDCA", Plan-Do-Check-Act) aportarà molts beneficis i ens permetrà aproximar-nos a l'excel·lència en termes de seguretat de la informació.

Dintre de l'entorn de la seguretat, es molt comú dir que la seguretat és com una cadena, i es ben conegut que *"una cadena és tan forta com la seva baula més feble",* per tant podem veure clarament que la confecció del nostre PDS ens permetrà **analitzar l'estat complert de tot el conjunt**, es a dir la situació de totes les nostres baules; de cara a poder **conèixer quines son les debilitats presents** i **poder decidir d'una forma no arbitraria i amb arguments** en quins punts hem de reforçar-la o fins i tot conèixer on es pot trencar per estar preparats de de cara a una ràpida resolució. Aquesta continua avaluació de la situació i evolució en el mon de la seguretat de la informació ens aproximarà a una situació de control i preparació de cara a les possibles situacions que es puguin donar al futur i que puguin impactar sobre la nostra informació o els propis sistemes de la informació. Aprofitant el nostre exemple de la cadena, veiem clarament, que la seguretat de la informació es una tasca de tots els departaments de l'organització i que ens permetrà reforçar tots els punts relacionats i no només en termes de sistemes informàtics.

No em d'oblidar mai, que estar segur al 100% és un concepte impossible, i en la seguretat de la nostra informació es dona aquesta situació, però la confecció d'aquest PDS ens permetrà elevar al màxim de les nostres possibilitats el nivell de seguretat i estar preparats per la resta d'esdeveniments, ja que els coneixent, contra els que no hem pogut assegurar-nos. (concepte de "risc residual" que es pot trobar al glossari d'aquest document).

2.1.- NECESSITAT DEL PLA DIRECTOR

Una vegada que ja coneixem en que consisteix un PDS i que aporta, anem a situar-nos molt més concretament en la nostra organització i veurem diferents punts més concrets que ens podem ajudar a tots a comprendre la necessitat del PDS dintre de la nostre organització. De cara a veure aquest punt concrets, realitzarem aquesta visió realitzant tot una sèrie de qüestions relacionades que ara mateix no coneixem la resposta i que el PDS en ajudarà a conèixer. Gracies a aquestes qüestions exemple, des de tots els departament podrem veure concretament quina es la utilitat i per tant es permetrà argumentar la seva necessitats.

La qüestions que avui dia no tenen resposta i gracies al PDS podrem conèixer, podríem ser de l'estil a:

- 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?

Aquestes preguntes exemples, i moltes d'altres que es podríem formular a mode d'exemple tant a nivell dels sistemes informàtics com als diferents departaments de la societat, posem de manifest que una de les premisses de cara a estar segur en tot moment es poder conèixer, valorar, quantificar, ràpidament la situació actual de cara a poder prendre mesures i decisions per tal de minimitzar aquestes possibles amenaces a les que podem estar exposats o tenir clar quin es el risc al que ens exposem i com poder reaccionar en cas de materialitzar-se.

Com veiem clarament, la realització d'aquest PDS, que es basarà en la realització, e iteració de tot el procés complert, d'un **anàlisi de riscos**, per avaluar la situació i poder optar per millores o projectes a implementar de cara a reduir aquests riscos ens permetrà respondre a les preguntes:

- Què cal protegir?

- De quin o de qui i, per què?

- Com protegir?

- Que es pot fer per evitar? Mereix la pena realitzar aquesta millora?

- Quin impacte tindria sobre la nostra organització.....?

2.1.1.- BENEFICIS DEL PLA DIRECTOR

Dels apartats anteriors ja es podem deduir o inclús observar clarament tot una sèrie de beneficis que aporta la realització d'aquest PDS, i que no em d'oblidar que es tracta del punt de partida d'un procés iteratiu i evolutiu en el temps on l'objectiu principal és millorar constantment en la seguretat de la informació de la nostra societat. A la seva vegada la confecció del PDS ens permetrà desenvolupar:

- 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.

Si donem un pas més en profunditat, podem veure que la realització del PDS i la seva posterior recurrència tant per controlar con per evolucionar la situació ens permetrà cobrir qualsevol dels objectius següents:

- Formular els requisits i objectius de seguretat de la informació de la nostra organització.
- Assegurar que els riscos de seguretat es gestionen de manera efectiva en termes de costos.
- Assegurar el compliment de lleis i regulacions vigents.
- Implementar i gestionar els controls necessaris per a assegurar que s'aconsegueixen els objectius de seguretat que ha definit l'organització.
- Definir nous processos de gestió de la seguretat, o identificar i aclarir els processos que ja hi ha.
- Implicar tant la direcció com la resta de departaments de l'organització en l'estat de les activitats de gestió de la seguretat ja que es tracta d'un benefici comú.
- 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.

2.1.2.- IMPACTE DEL PLA DIRECTOR SOBRE L'ORGANITZACIÓ

Evidentment, tot i els beneficis presentats en l'apartat anterior i que tots els departaments valoraran de forma molt positiva, presenta un impacte directe sobre l'organització que resulta important avançar en aquest moment per tal de tenir tots clars quines seran les necessitats i obligacions que acompanyaran a la realització d'aquest PDS.

D'entrada es clar que la confecció d'aquest PDS, suposarà una carga de treball sobre el personal implicat i la col·laboració de gran part del personal de l'organització de cara a plasmar la situació real i poder d'aquesta forma realitzar un anàlisi de riscos el mes aproximat a la realitat i amb les valoracions més exactes possibles, dintre de la mesura del possible.

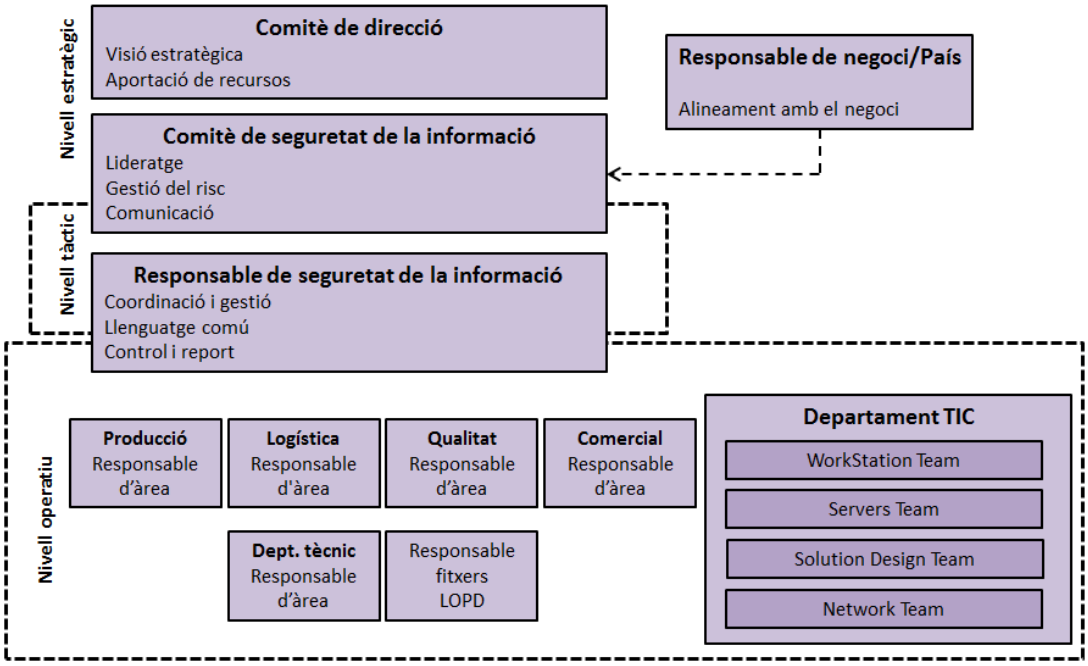
Per l'altre cantó: es molt probable que per tal de garantir la seguretat de la informació s'hagin d'establir uns procediments d'actuació o de treball amb els sistemes de la informació que a priori podem ser diferents de la metodologia actual i podem semblar més complicats o menys eficients inicialment però hem de considera que a vegades aquesta eficiència que podem estar implementant actualment pot anar contra la pròpia seguretat de la informació.

Per últim, el darrer aspecte que inicialment podem comentar que pot semblar un impacte sobre la metodologia actual de treball dels diferents departaments de l'organització, pot estar la pròpia coordinació amb l'equip de treball (organigrama que veurem en els següents apartats) en els aspectes relacionats amb la seguretat de la informació ja que es pot considerar com una pèrdua d'agilitat a l'hora d'implementar canvis o noves solucions però simplement cal recordar que la seguretat de la informació es una tasca transversal a tota l'organització i aquesta pèrdua d'agilitat vindrà recompensada amb una seguretat global que abans no es presentava.

2.2.- ORGANITZACIÓ I SEGUIMENT DEL PLA DIRECTOR

2.2.1.- ORGANITZACIÓ

De cara a garantir el bon resultat en la realització d'aquest PDS, i basant-nos en l'idea principal; que tots els esforços en matèria de seguretat de la informació seran inútils o molt poc eficaços si la companyia no té clar conceptes bàsics con perquè serveix, o qui té autoritat, sobre quins aspectes i qui és responsable de quines tasques o de quins àmbits; caldrà crear una estructura interna amb responsabilitat directa sobre la seguretat de la informació. Aquesta estructura, en el nostre cas concret quedaria de la següent manera:



A continuació, i basant-nos en l'esquema d'organització que acabem de presentar; definirem de manera molt ràpida les tasques més importants a realitzar per cada nivell ja que de cara a obtenir un bon resultat en la realització d'aquest PDS; resulta de vital importància conèixer quina es la missió de tots els participants.

El **comitè de direcció** presenta les següents funcions:

- Fer de la seguretat de la informació un punt de l'agenda del comitè de direcció de la companyia.
- Nomenar els membres d'un comitè de seguretat de la informació i donar-hi suport, dotar-lo dels recursos necessaris i establir-hi les directrius de treball.
- Aprovar la política, les normes i responsabilitats generals en matèria de seguretat de la informació.
- Determinar el llindar de risc acceptable en matèria de seguretat.
- Analitzar riscos possibles introduïts per canvis en les funcions o en el funcionament de la companyia per a adoptar les mesures de seguretat més adequades.

- Aprovar el pla de seguretat de la informació, que recull els principals projectes i iniciatives en la matèria.
- Fer el seguiment del quadre de comandament de la seguretat de la informació.

El **comitè de seguretat de la informació** s'encarregarà de:

- Implantar les directrius del comitè de direcció.
- Assignar rols i funcions en matèria de seguretat.
- Presentar a aprovació al comitè de direcció les polítiques, normes i responsabilitats en matèria de seguretat de la informació.
- Validar el mapa de riscos i les accions de mitigació que han proposat el responsable de seguretat de la informació.
- Validar el pla de seguretat de la informació (PDS) i presentar-lo a aprovació al comitè de direcció. Supervisar-ne la implantació i fer-ne el seguiment.
- Supervisar i aprovar el desenvolupament i manteniment del pla de continuïtat de negoci.
- Vetllar perquè es compleixi la legislació que sigui aplicable en matèria de seguretat.
- Promoure la conscienciació i formació d'usuaris i liderar la comunicació necessària.
- Revisar les incidències més destacades.
- Aprovar i revisar periòdicament el quadre de comandament de la seguretat de la informació i de l'evolució de l'SGSI.

La figura del **Responsable de seguretat de la informació (RSI)** que serà la persona encarregada de confeccionar aquest PDS, s'encarregarà de:

- Implantar les directrius del comitè de seguretat de la informació de la companyia.
- Elaborar, promoure i mantenir una política de seguretat de la informació, i proposar anualment objectius/projectes per millorar el nostre PDS.
- Actuar com a punt focal en matèria de seguretat de la informació dins de la companyia, cosa que inclou la coordinació amb altres unitats i funcions, a fi de gestionar la seguretat de la informació de manera global.
- Promoure i coordinar entre les àrees de negoci l'anàlisi de riscos dels processos més crítics i la informació més sensible, i proposar accions per a millorar i mitigar el risc, d'acord amb el llindar acceptable que ha definit el comitè de direcció. Elevar el mapa de riscos i el pla de seguretat de la informació al comitè de seguretat de la informació (CSI).
- Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.
- Revisar periòdicament l'estat de la seguretat en qüestions organitzatives, tècniques o metodològiques.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat

dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Vetllar pel compliment legal.
- Definir l'arquitectura de seguretat dels sistemes d'informació, monitorar la seguretat en l'àmbit tecnològic, fer el seguiment de les incidències de seguretat i escalar-les al CSI si correspon.
- Elaborar i mantenir un pla de conscienciació i formació en seguretat de la informació del personal, en col·laboració amb la unitat responsable de formació de la companyia.
- Coordinar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament per garantir la correcta evolució en la creació d'aquest PDS.

A continuació, definirem de forma genèrica algunes de les tasques a realitzar pel **nivell operatiu** que al cap i a la fi, es on trobarem els perfils més actius dintre de la creació d'aquest PDS, d'una banda aportant el coneixement a l'hora d'implementar un document d'aquest tipus i la relació amb la part tècnica, aportada pels diferents equips del departament de tecnologia i sistemes de la informació i d'altre banda la visió del responsable/usuaris avançats dels diferents departaments implicats, que aportaran la relació i la importància d'aquest PDS amb l'organització i el seu departament concret. Es molt habitual que les valoracions siguin formulades directament per aquestes persones ja que coneixen directament l'impacte sobre els seus departaments de les diferents suposicions.

Per tant podríem trobar les següents tasques (entre d'altres):

- Classificar la informació de la qual són responsables segons la criticitat que aquesta tingui per a la companyia en termes de confidencialitat, privadesa, integritat, continuïtat, autenticitat, no-repudi, traçabilitat i impacte mediàtic i determinar l'ús que s'ha de fer de la informació i qui hi pot accedir.
- Tenir coneixement de la normativa general o sectorial aplicable a la informació de la qual són responsables, inclosa la normativa vigent en matèria de protecció de dades de caràcter personal.
- Fer el seguiment de l'estat de la seguretat dels sistemes d'informació que tractin la informació de què són responsables i gestionar la mitigació de riscos dins del seu nivell de decisió.
- Implicar-s'hi i definir procediments alternatius en cas d'indisponiblitat del sistema o falta d'integritat de la informació.
- Col·laborar a fer revisions i el seguiment durant la realització d'aquest PDS.
- Complir les polítiques, les normes i els procediments en matèria de seguretat de la informació. Col·laborar amb l'RSI a definir-los.
- Implantar en els sistemes d'informació els controls de seguretat prescrits i les accions correctores establertes i gestionar les vulnerabilitats detectades.
- Requerir la participació de l'RSI en la implantació o gestió dels canvis de programari per tal de mitigar el riscos descoberts.
- Col·laborar amb l'RSI a identificar riscos i a proposar solucions, i col·laborar en les revisions o auditories de seguretat que es duguin a terme.

2.2.2.- SEGUIMENT

Com em pogut observar en una de les tasques del responsable de seguretat de la informació; s'ha de revisar periòdicament tant l'evolució en el moment de la realització del PDS com posteriorment en el seu manteniment i evolució per tal de permetre proposar o actualitzar el PDS i incorporar-hi totes les accions preventives, correctives i de millora que s'han anat detectant. Una vegada el CSI ha aprovat aquest pla (i el pressupost corresponent); l'RSI ha de gestionar el pressupost assignat i la contractació de recursos quan sigui necessari.

Per tant, per tal de garantir aquest seguiment durant la primera fase, la creació del PDS; establirem un punts de control durant tota la realització d'aquest PDS per tal de garantir la correcte evolució en el temps planificat o poder abordar ràpidament i de manera àgil els diferents problemes que puguin sorgir durant les diferents fases.

De cara a establir aquest punts, fixarem un control a la meitat de cada fase, i a la finalització de la mateixa per tal de visionar l'estatus de la mateixa. Les fases concretes seran:

- **FASE 1:** Estat del risc: Identificació i valoració dels actius i amenaces.
- **FASE 2:** Auditoria de compliment de la ISO:IEC 27002:2005
- **FASE 3:** Proposta de projectes
- **FASE 4:** Presentació del resultat i planificació futura.

Evidentment, durant la realització de cada fase, el RSI s'encarregarà de realitzar el corresponent seguiment i en cas de detectar qualsevol problema que necessiti la decisió o l'aportació del comitè de seguretat o el propi comitè de direcció; s'encarregarà d'elevar i presentar aquesta situació.

Dintre de les funcions del RSI, es troba la realització d'un fitxer d'estatus que anirà complimentant amb la informació recopilada als punts de control i possibles tasques especifiques de cada apartat que es vulguin controlar amb més detall de cara a poder presentar aquesta correcta evolució al comitè de seguretat. Es definiran tot una sèrie de plantilles a complimentar les diferents participants del PDS, per tal de recopilar la informació necessària per a cada punt de control.

A la vegada, es prepararà un document per declarar possibles problemes en qualsevol moment que es trobarà a la disposició de tots els integrants de la realització d'aquest PDS, per tal de poder gestionar ràpidament les adversitats que puguin ocorre.

2.3.- RECURSOS PEL PLA DIRECTOR

En aquest apartat, com en el seus subapartats, veurem totes les necessitats recursos inicials que podem detectar seran necessaris per la realització d'aquest PDS; i molt important (encara podríem dir que molt més important que la pròpia confecció inicial del PDS); els recursos necessaris per mantenir actiu aquest PDS i la seva evolució posterior de cara a anar aplicant les tècniques de millora continua sobre aquest PDS per arribar a evolucionar tant com sigui possible la seguretat de la informació de la nostra societat.

A la vegada, s'inclou un apartat dedicat a indicar el procediment a seguir de cara a sol·licitar recursos que no hagin estat indicats en aquesta previsió inicial i el seu procediment de validació.

2.3.1.- ESPONSORITZACIÓ DEL PLA

Amb l'objectiu de garantir la correcta realització d'aquest PDS, i basant-nos en l'organització i tasques que hem pogut observar en els apartats anteriors que impliquen la col·laboració de tots els departaments de la nostra societat; resulta indispensable que la direcció aprovi la realització d'aquest PDS, con l'estructura organitzativa i l'assignació de funcions de seguretat i hi doni suport, per a dotat les persones amb responsabilitat en la matèria de l'autoritat i el temps necessaris per a exercir les seves funcions dins de la companyia.

Aquesta validació i suport per part de la direcció quedarà plasmada en un document inicial que s'utilitzarà en el moment de la presentació del PDS als diferents departaments de la societat, on s'indicarà el tipus de col·laboració que s'haurà de rebre de cada departament o persona concret i com serà la seva implicació dintre del projecte.

Es molt important que en el moment d'aquesta presentació del PDS que anem a realitzar per la societat, a part de veure el propi suport de la direcció de la societat, es pugui veure clarament la funcionalitat i utilitat que tindrà per tothom i s'ha de aconseguir implicar i motivar a tots els actors necessaris per la realització, de cara a que estiguin motivats amb la seva implicació.

2.3.2.- RECURSOS ORGANITZATIUS

Tal com hem pogut observar en l'organigrama de l'organització de l'estructura necessària per la realització d'aquest PDS, s'haurà de disposar de diferents perfils dintre dels diferents departaments de l'organització, per tal garantir la realització d'aquest PDS i el seu corresponent manteniment i evolució.

Una vegada la creació d'aquest PDS estigui validada i presentada pel comitè de direcció, es procedirà a crear un document que s'annexarà a la documentació del PDS indicant les persones concretes de cada departament que hauran de participar en el projecte per garantir les diferents tasques que hem vist en el de l'organització d'aquest document.

2.3.3.- RECURSOS MATERIALS

Per la realització d'aquest PDS, a priori, no es necessitarà cap tipus de material específic que es trobi fora del propi equip i medis de treball de les persones assignades al projecte i per tant no detectem cap necessitat inicial per la realització. Si a mesura que anem avançant es detectes qualsevol tipus de necessitat, es procediria a activar el procediment de sol·licitud de recursos que tot seguit comentarem.

2.3.4.- SOL·LICITUD DE RECURSOS

De cara a la sol·licitud extra durant la confecció, realització, implantació i posterior iteració d'aquest PDS, s'haurà de realitzar una petició directa al RSI, indicant i justificant la necessitat d'aquest recursos, per tal de poder decidir per part del RSI, si son assignats (o no) o si es necessari elevar la petició al comitè de direcció. L'interlocutor amb el comitè de direcció en aquest cas serà directament el propi RSI.

3.- ESTAT DEL RISC: Identificació i Valoració dels Actius i Amenaces

3.1.- Introducció

En aquesta fase del document, l'objectiu es poder avaluar tots els actius que es troben relacionats amb la creació del nostre PDS, considerant les dependències existents entre ells i realitzant una valoració dels mateixos. D'aquesta forma tindrem clarament una situació de partida a nivell de tots els actius, ja siguin tangibles o no, dintre de la societat i podrem analitzar a quines amenaces podem estar exposats aquest actius. Per últim, un com tinguem les amenaces reals que poden afectar als nostres actius, estarem en disposició de poder realitzar la avaluació de l'impacte que sofriria l'organització en cas de que aquestes amenaces es materialitzessin.

Com tots podem intuir, aquest càlcul de l'impacte resultarà una dada rellevant, ja que permetrà prioritzar el pla d'acció, i alhora, avaluar com es veu modificat aquest valor un cop s'apliquin contramesures o fins i tot tenir coneixement en tot moment quin es el risc assumit (risc residual) que estem disposats suportar per la nostra organització ja sigui per la no implantació de contramesures o pel fet que les mesures no puguin descartar l'amenaça al 100%.

Gracies a aquesta fase del PDS, obtindrem:

- 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.

3.2.- Inventari d'actius

De cara a poder procedir a realitzar aquest anàlisi i avaluació comentat a la introducció d'aquest apartat, el primer pas que hem de realitzar serà identificar tots els actius vinculats a la informació. De cara a poder clarificar aquesta identificació, i tal com realitza la metodologia MAGERIT, procedirem a agrupar els actius d'acord a les següents agrupacions (en funció del àmbit del actiu):

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

De cara a evitar repetir aquesta taula tant en aquest punt con en els dos punts posteriors, plasmarem el resultat d'aquesta primera fase en la taula resum que podem observar en el

apartat 3.5 d'aquest mateix document. La primera columna de la taula, on trobem l'àmbit de l'actiu per realitzar les agrupacions i la segona columna on trobem l'actiu concret al que fent referencia; correspondrien al resultat d'aquest inventari d'actius.

3.3.- Valoració dels actius

Una vegada hem procedit a la identificació mitjançant l'inventari d'actius en relació a la seguretat de la informació, caldrà valorarà cada actiu dintre de la nostre organització. Si pensem en el procés en conjunt, l'objectiu final és prendre un conjunt de mesures que garanteixin els nostres actius. El sentit comú indica que el cost de les mesures no ha de ser superior al cost de l'actiu protegit, per tant veiem que resulta vital per poder avançar, determinar el valor dels diferents actius.

De cara a poder realitzar aquesta valoració, com tots coneixem, no resulta una tasca fàcil poder donar una xifra final que identifiqui el valor del actiu, ja que s'han de tenir en compte molts conceptes com per exemple el cost de reposició, el valor del temps sense servei, possible penalitzacions, cost equip de resolució, etc. A aquesta dificultat haurem de sumar quan es tracta d'un actiu intangible on efectuar la valoració quantitativa resulta molt més complicat encara (per exemple, quants euros val la pèrdua de la Base de Dates de clients???). Per tant, per tal de poder facilitar aquesta tasca, i tal com es proposa a la metodologia MAGERIT, procedirem a realitzar una valoració qualitativa, en relació al valor que te l'actiu respecte la nostre organització, la qual completarem amb una valoració quantitativa respecte aquestes categories qualitatives:

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€

Gracies a aquesta taula podrem realitzar l'assignació d'un valor als actius en funció de les categories de la columna "Valoració" i a la seva vegada tindrem un valor quantitatiu que ve representat a la columna "Valor". Com podem imaginar en alguns casos el "valor" quantitatiu assignat serà superior (o inferior) al valor real que seria molt laboriós d'obtenir, però gracies al rang en el que es troba l'actiu, podrem estimar amb certa precisió el valor dels actius.

Addicionalment, cal tenir en compte que els actius estan en realitat jerarquitzats. És a dir, hem d'identificar i valorar les dependències entre actius. *Es diu que 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.* O dit en altres paraules, quan la materialització d'una amenaça en l'actiu inferior és un perjudici sobre l'actiu superior. Per tant haurem d'identificar

clarament l'arbre de dependències o jerarquia entre els actius existents e identificats a la nostra organització.

De cara a establir aquesta dependències d'una forma visual molt clara i rapida de comprendre sobre la pròpia taula que trobem a l'apartat 3.5 d'aquest document, trobarem la columna "Dependència" al costat de la columna "Actiu", on reflectirem els actius inferiors de cada actiu, o dit d'altre forma, veurem la llista d'actius sobre els quals una amenaça afectarà a l'actiu superior.

3.4.- Dimensions de seguretat

Un cop identificats els actius, amb les seves dependències, i la seva valoració; haurem de realitzar la valoració de la criticitat en les cinc dimensions de la seguretat de la informació manejada pel procés de negoci de la nostra organització. Evidentment aquesta valoració de la criticitat ens serà d'ajuda en el moment de pensar en possibles salvaguardes, ja que aquestes s'enfocaran als aspectes que més ens interessin.

Les 5 dimensions de les que estem parlant són:

- **[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.

Aquesta valoració en les 5 dimensions, ens permetrà a posteriori valorar el impacte que tindrà la materialització d'una amenaça sobre la part d'actiu exposat (no cobert per les salvaguardes en cadascuna de les dimensions).

Un cop explicades les cinc dimensions s'ha de tenir present l'escala en què es realitzaran les valoracions. En aquest cas utilitzarem una escala de valoració de deu valors seguint els següents criteris:

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

De cara a la valoració d'aquestes 5 dimensions caldrà tindre en compte les dependències entre actius i per tant per aquestes valoracions parlarem que aquest valor serà **propi o acumulat. El valor propi s'assignarà a la informació,** quedant els altres actius subordinats a les necessitats

d'explotació i protecció de la informació. Així doncs, **els actius inferiors en un esquema de dependències acumulen el valor dels actius que es recolzen en ells.** Cada actiu d'informació pot tenir un valor diferent en cadascuna de les diferents dimensions per la nostra organització, per això hem de tenir present sempre que representa cada dimensió.

Per acabar d'entendre clarament aquesta valoració amb els actius dependents, indicaré un exemple ràpid de cara a fer mes comprensible els valors observats a la taula del apartat 3.5

- Exemple de dependència i valoració:
  - Tenim com actius:
    - Servidor (A)
    - Aplicació (B)
    - Dades de la aplicació (C)
  - Assumim que:
    - L'aplicació sense dades no te cap valor.
    - Les dades sense aplicació no podem ser explotades.
  - Per tant veuríem que les dependències d'actius serien:
    - B depèn de A i C
    - C depèn de A i B

> ➢ Si per exemple valoressin la "accessibilitat" de les dades amb un 7 (**valor propi**); podríem dir aplicant que tant A com B mantindríem aquesta valoració **ja que son actius inferiors de l'actiu de la informació** (C) que estem valorant.

3.5.- Taula resum de la valoració

A continuació trobem la taula resum on podem observar l'inventari dels actius de l'organització en funció del seu àmbit, la relació d'actius inferiors dels qual depèn, la seva valoració a nivell de l'organització i per últim la valoració de les cinc dimensions de la seguretat de la informació manejada pel procés de negoci:

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.2]	Sala comunicacions HQ ES		A	8	8	10	9	8
	[L.3]	Sala comunicacions HQ PT		A	8	8	10	9	8
	[L.4]	Sala comunicacions FAB		MA	8	9	10	9	9
	[L.5]	Sala comunicacions CD ES		M	5	8	10	7	5
	[L.6]	Sala comunicacions CD PT		M	5	8	10	7	5
[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.2]	Servidor Correu Front-End [SRVMAD13]	[L.1] - [HW.1] - [HW.3] [HW.4] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [D.13]	MB	8	7	8	6	6
	[HW.3]	AntiSpam 1 [IronPort1]	[L.1] - [HW.21] - [COM.17] [COM.18] - [COM.19] - [COM.20]	MB	8	7	8	6	6
	[HW.4]	AntiSpam 2 [IronPort2]	[L.1] - [HW.21] - [COM.17] [COM.18] - [COM.19] - [COM.20]	MB	8	7	8	6	6
	[HW.5]	Servidor DC/FS/Exchange [ESWK3COR902]	[L.2] - [HW.22] - [COM.21] [COM.22] - [COM.23] - [COM.24] [D.14] - [D.13]	MB	8	8	8	6	6
	[HW.6]	Servidor DC/FS/Exchange PT [PTWK3CAR902]	[L.3] - [HW.23] - [COM.25] [COM.26] - [COM.27] - [COM.28] [D.15] - [D.13]	MB	8	8	8	6	6

	[HW.7]	Servidor COM [ESWK3MAD905]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [SI.8]	MB					
	[HW.8]	Servidor COM [ESWK3MAD906]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [SI.9]	MB					
	[HW.9]	Chasis BLADE	[HW.21] - [COM.1] - [COM.2] [COM.3] - [COM.4] - [SI.1] [HW.10] - [HW.11] - [HW.12]	M	8	8	9	6	6
	[HW.10]	Servidor Web [SRVMAD21]	[L.1] - [HW.21] - [HW.9] [COM.1] - [COM.2] - [COM.3] [COM.4] - [D.16]	B	8	8	9	6	6
	[HW.11]	Servidor Web [SRVMAD22]	[L.1] - [HW.21] - [HW.9] [COM.1] - [COM.2] - [COM.3] [COM.4] - [D.16]	B	8	8	9	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.14]	Servidor Antivirus [SRVMAD03]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4]	MB					
	[HW.15]	Servidor Firewall [SRVMAD12]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4]	MB					
	[HW.16]	Servidor Aplicacions [SRVMAD05]	[SW.1] - [SW.3] - [SW.4] - [SW.5] [L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [D.11]	MB	7	9	8	9	9

	[HW.17]	Servidor INFOLOG [ESAS400]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [D.7]	A	5	8	10	7	5
	[HW.18]	Servidor 2 INFOLOF [ESAS400Rep]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [D.7]	A	5	8	10	7	5
	[HW.19]	Servidor Bases Dades [SRVMAD06]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [D.6] - [D.8] - [D.9] - [D10]	B	7	9	8	9	9
	[HW.20]	Servidor CALOR [SRVMAD07]	[L.1] - [HW.21] - [COM.1] [COM.2] - [COM.3] - [COM.4] [D.12]	MB	6	8	10	8	8
	[HW.21]	Switches LAN CPD	[L.1]	MB	8	9	10	9	9
	[HW.22]	Switches LAN HQ ES	[L.2]	MB	8	8	10	9	8
	[HW.23]	Switches LAN HQ PT	[L.3]	MB	8	8	10	9	8
	[HW.24]	Switches LAN FAB	[L.4]	MB	8	9	10	9	9
	[HW.25]	Switches LAN CD ES	[L.5]	MB	5	8	10	7	5
	[HW.26]	Switches LAN CD PT	[L.6]	MB	5	8	10	7	5
	[HW.27]	Terminals Lectura SGANL	[HW.24] - [HW.25] - [HW.26]	B	5	7	8	5	5
	[HW.28]	Terminals Lectura INFOLOG	[HW.24] - [HW.25] - [HW.26]	B	5	8	10	7	5
	[HW29]	Acces Point SGANL	[HW.24] - [HW.25] - [HW.26]	MB	5	7	8	5	5
	[HW.30]	Acces Point 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
	[SW.3]	Aplicació SGANL	[HW.16]	B	5	7	8	5	5
	[SW.4]	Aplicació PRISMA	[HW.16]	B	3	7	4	3	3
	[SW.5]	Aplicació ORALIMS	[HW.16]	M	7	9	8	9	9
	[SW.6]	Aplicació CALOR	[HW.20]	A	6	8	10	8	8

[D] - Dades/Info.	**[D.1]**	Dades pròpies Intranet	[SI.1] - [HW.9]	M	**8**	**8**	**6**	**9**	**7**
	[D.2]	Dades web Marca X	[SI.1] - [HW.9]	B	**6**	**7**	**5**	**4**	**4**
	[D.3]	Dades web Marca Y	[SI.1] - [HW.9]	B	**6**	**7**	**5**	**4**	**4**
	[D.4]	Dades web Marca Z	[SI.1] - [HW.9]	B	**6**	**7**	**5**	**4**	**4**
	[D.5]	Dades web Promoció 2X	[SI.1] - [HW.9]	B	**6**	**7**	**5**	**4**	**4**
	[D.6]	Dades SKEP	[SI.18] - [HW.19] - [SW.1]	A	**5**	**9**	**7**	**7**	**5**
	[D.7]	Dades INFOLOG	[SI.14] - [SI.16] - [HW.17] [HW.18] - [SW.2]	MA	**5**	**8**	**10**	**7**	**5**
	[D.8]	Dades SGANL	[SI.18] - [HW.19] - [SW.3]	M	**5**	**7**	**8**	**5**	**5**
	[D.9]	Dades PRISMA	[SI.18] - [HW.19] - [SW.4]	B	**3**	**7**	**4**	**3**	**3**
	[D.10]	Dades ORALIMS	[SI.18] - [HW.19] - [SW.5]	A	**7**	**9**	**8**	**9**	**9**
	[D.11]	Dades Intercanvi ORALIMS	[SI.13] - [HW.16]	MB	**3**	**3**	**4**	**2**	**2**
	[D.12]	Dades CALOR	[SI.18] - [SI.19] - [HW.20] - [SW.6]	MA	**6**	**8**	**10**	**8**	**8**
	[D.13]	BD servidor de Correu	[SI.2] - [HW.1]	M	**8**	**7**	**8**	**6**	**6**
	[D.14]	Dades FileServer HQ ES	[SI.4] - [HW.5]	A	**6**	**8**	**7**	**4**	**4**
	[D.15]	Dades FileServer HQ PT	[SI.6] - [HW.6]	A	**6**	**8**	**7**	**4**	**4**
	[D.16]	Dades Cabina de Discos	[SI.1]	M	**8**	**8**	**9**	**6**	**6**
[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
	[COM.3]	Router Backup CPD ES	[L.1]	MB	8	9	10	9	9
	[COM.4]	Línia Baclup CPD ES	[L.1]	MB	8	9	10	9	9
	[COM.5]	Router Primari Connexió FR	[L.1]	MB					
	[COM.6]	Línia 1 Connexió FR	[L.1]	MB					
	[COM.7]	Router Backup Connexió FR	[L.1]	MB					
	[COM.8]	Línia 2 Connexió FR	[L.1]	MB					
	[COM.9]	Router Primari Connexió FR (2)	[L.1]	MB					

[COM.10]	Línia 3 Connexió FR	[L.1]	MB						
[COM.11]	Router Backup Connexió FR (2)	[L.1]	MB						
[COM.12]	Línia 4 Connexió FR	[L.1]	MB						
[COM.13]	Router Primari Connexió IT	[L.1]	MB						
[COM.14]	Línia Principal IT	[L.1]	MB						
[COM.15]	Router Backup Connexió IT	[L.1]	MB						
[COM.16]	Línia Backup IT	[L.1]	MB						
[COM.17]	Router Primari Internet	[L.1]	MB						
[COM.18]	Línia Principal Internet	[L.1]	MB						
[COM.19]	Router Secundari Internet	[L.1]	MB						
[COM.20]	Línia Backup Internet	[L.1]	MB						
[COM.21]	Router Primari HQ ES	[L.2]	MB	8	8	10	9	8	
[COM.22]	Línia Principal HQ ES	[L.2]	MB	8	8	10	9	8	
[COM.23]	Router Backup HQ ES	[L.2]	MB	8	8	10	9	8	
[COM.24]	Línia Backup HQ ES	[L.2]	MB	8	8	10	9	8	
[COM.25]	Router Primari HQ PT	[L.3]	MB	8	8	10	9	8	
[COM.26]	Línia Principal HQ PT	[L.3]	MB	8	8	10	9	8	
[COM.27]	Router Backup HQ PT	[L.3]	MB	8	8	10	9	8	
[COM.28]	Línia Backup HQ PT	[L.3]	MB	8	8	10	9	8	
[COM.29]	Router Primari Fàbrica	[L.4]	MB	8	9	10	9	9	
[COM.30]	Línia Primària FAB	[L.4]	MB	8	9	10	9	9	
[COM.31]	Router Backup Fàbrica	[L.4]	MB	8	9	10	9	9	
[COM.32]	Línia Backup FAB	[L.4]	MB	8	9	10	9	9	
[COM.33]	Router Primari CD ES	[L.5]	MB	5	8	10	7	5	
[COM.34]	Línia Primària CD ES	[L.5]	MB	5	8	10	7	5	
[COM.35]	Router Backup CD ES	[L.5]	MB	5	8	10	7	5	

	[COM.36]	Línia Backup CD ES	[L.5]	MB	5	8	10	7	5
	[COM.37]	Router Primari CD PT	[L.6]	MB	5	8	10	7	5
	[COM.38]	Línia Primària CD PT	[L.6]	MB	5	8	10	7	5
	[COM.39]	Router Backup CD PT	[L.6]	MB	5	8	10	7	5
	[COM.40]	Línia Backup CD PT	[L.6]	MB	5	8	10	7	5
[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 Acces 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
[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.2]	Discos Server [ESWK3MAD902]	[D.13] - [HW.1]	MB	8	7	8	6	6
	[SI.3]	Discos Server [SRVMAD13]	[D.13] - [HW.2]	MB	8	7	8	6	6
	[SI.4]	Discos Server [ESWK3COR902]	[D.14] - [HW.5]	MB	6	8	7	4	4
	[SI.5]	Cinta Backup [ESWK3COR902]	[SI.4]	MB	6	8	7	4	4
	[SI.6]	Discos Server [PTWK3CAR902]	[D.15] - [HW.6]	MB	6	8	7	4	4
	[SI.7]	Cinta Backup [PTWK3CAR902]	[SI.6]	MB	6	8	7	4	4
	[SI.8]	Discos Server [ESWK3MAD905]	[HW.7]	MB					
	[SI.9]	Discos Server [ESWK3MAD906]	[HW.8]	MB					
	[SI.10]	Discos Server [SRVMAD30]	[HW.13]	MB					
	[SI.11]	Discos Server [SRVMAD03]	[HW.14]	MB					
	[SI.12]	Discos Server [SRVMAD12]	[HW.15]	MB					
	[SI.13]	Discos Server [SRVMAD05]	[HW.16]	MB	7	9	8	9	9
	[SI.14]	Discos Server [ESAS400]	[D.7] - [HW.17]	MB	5	8	10	7	5
	[SI.15]	Cintes Backup [ESAS400]	[SI.14]	MB	5	8	10	7	5
	[SI.16]	Discos Server [ESAS400Rep]	[D.7] - [HW.18]	MB	5	8	10	7	5
	[SI.17]	Cintes Backup [ESAS400Rep]	[SI.16]	MB	5	8	10	7	5
	[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.3]	Equip Antiincendi CPD	[L.1]	B	8	9	10	9	9

	[AUX.4]	Control Acces CPD	[L.1]	MB	8	9	10	9	9
	[AUX.5]	Caixa Forta CPD	[L.1]	MB	8	9	10	9	9
	[AUX.6]	UPS pel FAB	[L.4]	B	8	9	10	9	9
	[AUX.7]	Equip climatització FAB	[L.4]	B	8	9	10	9	9
	[AUX.8]	Equip Antiincendi FAB	[L.4]	B	8	9	10	9	9
	[AUX.9]	Control Acces FAB	[L.4]	MB	8	9	10	9	9
	[AUX.10]	Generador Elèctric FAB	[L.4]	A	8	9	10	9	9
	[AUX.11]	UPS HQ ES	[L.2]	MB	8	8	10	9	8
	[AUX.12]	Climatització HQ ES	[L.2]	MB	8	8	10	9	8
	[AUX.13]	UPS HQ PT	[L.3]	MB	8	8	10	9	8
	[AUX.14]	Climatització HQ PT	[L.3]	MB	8	8	10	9	8
	[AUX.15]	UPS CD ES	[L.5]	MB	5	8	10	7	5
	[AUX.16]	UPS CD PT	[L.6]	MB	5	8	10	7	5
[P] - Personal	**[P.1]**	Responsable de Seguretat		M					
	[P.2]	Responsable de Xarxa		M					
	[P.3]	Tècnic Xarxa		MB					
	[P.4]	Responsable de Servidors		M					
	[P.5]	Tècnic Servidors		MB					
	[P.6]	Responsable d'aplicació		B					
	[P.7]	Tècnic Operacions		MB					
	[P.8]	Tècnic Operacions		MB					
	[P.9]	Responsable Bases de Dades		B					

* NOTES ACLARATORIES:

- De cara a fer més comprensibles les dependències dels actius, i evitar dependències cícliques que complicaríem massa la interpretació d'aquesta taula; hem decidit seguir les següents normes per instaurar les dependències de cada agrupació, tot i que, **les dependències que presenten els actius inferiors; seran dependències inferiors també del superior del primer actiu:**

    - **Instal·lacions.** No presentarà dependències.
    - **Hardware.** Dependrà directament (e indirectament dels seus inferiors):
        - Instal·lacions
        - Hardware
        - Comunicacions
        - Aplicació
        - Dades
    - **Aplicació.** Dependrà directament (e indirectament dels seus inferiors):
        - Hardware
    - **Dades.** Dependrà directament (e indirectament dels seus inferiors):
        - Suports
        - Hardware
        - Aplicació
    - **Comunicacions.** Dependrà directament (e indirectament dels seus inferiors):
        - Instal·lacions
    - **Servei.** Dependrà directament (e indirectament dels seus inferiors):
        - Aplicació
    - **Suports.** Dependrà directament (e indirectament dels seus inferiors):
        - Dades
        - Hardware
    - **Actius Auxiliars.** Dependrà directament (e indirectament dels seus inferiors):
        - Instal·lacions
    - **Actius Personal.** No presenta dependències.

- La valoració dels "Aspectes Crítics", es a dir les 5 dimensions de seguretat, s'ha realitzat mitjançant la informació obtinguda de la pròpia empresa mitjançant la documentació aportada en l'apartat 1 d'aquest document **i les posteriors consultes realitzades als responsables dels diferents departaments** per poder conèixer les valoracions per aquestes 5 dimensions. Un cop hem valorat els actius de l'agrupació "Dades/Informació" mitjançant les dependències en procedit a extrapolar aquest valors a la resta d'actius relacionats.

3.6.- Anàlisis d'amenaces

Els actius estan exposats a amenaces. Aquestes amenaces poden afectar els diferents aspectes de la seguretat. A nivell metodològic, volem analitzar quines amenaces poden afectar quins actius, i un cop estudiat, estimar com de vulnerable és l'actiu a la materialització de l'amenaça així com la freqüència estimada d'aquesta.

Al igual que en apartats anteriors, utilitzarem les amenaces més comuns conegudes i documentades a la metodologia MAGERIT pels actius que tenim a l'organització i que hem pogut observar a la taula de l'apartat 3.5

Aquestes amenaces les classificarem dintre de les següents agrupacions:

- Desastres Naturals [N."x"]
- D'origen industrial [I."x"]
- Error i fallades no intencionades [E."x"]
- Atacs intencionades [A."x"]

De cara a valorar la freqüència amb la que teòricament es pot materialitzar l'amenaça (en alguns casos seran dades estadístiques en funció de la zona, el terreny, clima, etc. I en altres seran estimacions que farem en base a la nostra experiència) trobem que utilitzarem la següent escala per poder mesurar-lo:

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

*NOTA: Si la dada a la freqüència es pot donar amb més precisió (perquè es tingui documentada o informació al respecte) aquesta s'inclourà directament sobre la taula **en la mateixa escala** que hem comentat a la taula anterior (vegades per any).

Podem observar en aquesta classificació, que mitjançant aquesta taula podrem passar (com en casos anteriors) des d'una valoració qualitativa cap a una valoració quantitativa de cara a poder realitzar els càlculs pertinents.

Per últim caldrà estimar l'impacte que produirà la materialització de l'amenaça en cadascuna de les 5 dimensions de seguretat valorades pels actius en la taula de l'apartat 3.5. En aquest cas; l'escala que utilitzarem serà el **"Tan per cent"** d'impacte sobre la dimensió valorada:

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

Donat que l'abast d'aquest PDS (com es va veure a l'apartat 1.5.2) esta focalitzat als serveis proveïts als usuaris (tant comuns com concrets), realitzarem l'anàlisi d'amenaces sobre els actius de tipus "Servei" (excloent els serveis "S.2", "S.8", "S.9", "S.14" i "S.15") per tractar-se de serveis propis del departament de Sistemes de la informació o esta allotjats a l'estranger i per tant no presentaven valoració a les dimensions crítiques de la taula de l'apartat anterior).

Per tant i un cop aclarides les diferents escales de valoració, obtenim la següent taula:

ACTIU/AMENACES			FREQÜÈNCIA (X/365)	IMPACTE				
				C	I	D	A	T
[S.1]	**Servei de Correu Usuaris**			**85%**	**75%**	**100%**	**65%**	**85%**
	Errors d'usuari	[E.1]	35	0%	5%	5%	0%	0%
	Errors dels Administradors	[E.2]	5	20%	50%	75%	5%	50%
	Errors de monitorització (log)	[E.3]	10	0%	0%	0%	0%	75%
	Errors de configuració	[E.4]	25	20%	5%	1%	20%	50%
	Errors de [re-]encaminament	[E.9]	5	75%	20%	0%	30%	5%
	Errors de seqüencia	[E.10]	1	0%	5%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	40	0%	0%	100%	0%	0%
	Manipulació de la configuració	[A.4]	1	85%	75%	100%	50%	50%
	Suplantació de la identitat de l'usuari	[A.5]	15	70%	45%	0%	25%	0%
	Aprofitament dels privilegis d'accés	[A.6]	1	5%	5%	0%	0%	0%
	Usos no previstos	[A.7]	7	0%	0%	85%	0%	0%
	[Re-]encaminament de missatges	[A.9]	4	75%	50%	0%	50%	25%
	Alteració de la seqüencia	[A.10]	0	0%	1%	0%	0%	0%
	Accessos no autoritzats	[A.11]	10	85%	50%	0%	65%	0%
	Repudi	[A.13]	1	0%	0%	0%	0%	85%
	Denegació de servei	[A.24]	3	0%	0%	85%	0%	0%
[S.3]	**Servei Intranet**			**75%**	**75%**	**100%**	**50%**	**35%**
	Errors d'usuari	[E.1]	5	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	15	65%	75%	75%	50%	25%
	Errors de monitorització (log)	[E.3]	20	0%	0%	0%	0%	35%
	Errors de configuració	[E.4]	35	25%	40%	75%	50%	5%
	Errors de [re-]encaminament	[E.9]	1	1%	1%	0%	1%	1%
	Errors de seqüencia	[E.10]	1	0%	1%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	5	0%	0%	100%	0%	0%
	Manipulació de la configuració	[A.4]	5	75%	65%	90%	40%	35%
	Suplantació de la identitat de l'usuari	[A.5]	2	65%	25%	0%	50%	0%
	Aprofitament dels privilegis d'accés	[A.6]	1	5%	5%	0%	0%	0%
	Usos no previstos	[A.7]	10	0%	0%	65%	0%	0%
	[Re-]encaminament de missatges	[A.9]	1	1%	1%	0%	1%	1%
	Alteració de la seqüencia	[A.10]	1	0%	1%	0%	0%	0%
	Accessos no autoritzats	[A.11]	3	50%	35%	0%	50%	0%
	Repudi	[A.13]	1	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	2	0%	0%	100%	0%	0%

[S.4]	**Servei Web Marca [X]**			**85%**	**75%**	**100%**	**50%**	**75%**
	Errors d'usuari	[E.1]	5	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	15	65%	75%	75%	50%	25%
	Errors de monitorització (log)	[E.3]	20	0%	0%	0%	0%	35%
	Errors de configuració	[E.4]	35	25%	40%	75%	50%	5%
	Errors de [re-]encaminament	[E.9]	1	1%	1%	0%	1%	1%
	Errors de seqüencia	[E.10]	1	0%	1%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	5	0%	0%	100%	0%	0%
	Manipulació de la configuració	[A.4]	5	85%	65%	90%	40%	75%
	Suplantació de la identitat de l'usuari	[A.5]	20	65%	25%	0%	50%	0%
	Aprofitament dels privilegis d'accés	[A.6]	5	5%	75%	0%	0%	0%
	Usos no previstos	[A.7]	35	0%	0%	65%	0%	0%
	[Re-]encaminament de missatges	[A.9]	5	50%	15%	0%	1%	1%
	Alteració de la seqüencia	[A.10]	5	0%	1%	0%	0%	0%
	Accessos no autoritzats	[A.11]	30	50%	35%	0%	50%	0%
	Repudi	[A.13]	5	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	8	0%	0%	100%	0%	0%
[S.5]	**Servei Web Marca [Y]**			**85%**	**75%**	**100%**	**50%**	**75%**
	Errors d'usuari	[E.1]	5	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	15	65%	75%	75%	50%	25%
	Errors de monitorització (log)	[E.3]	20	0%	0%	0%	0%	35%
	Errors de configuració	[E.4]	35	25%	40%	75%	50%	5%
	Errors de [re-]encaminament	[E.9]	1	1%	1%	0%	1%	1%
	Errors de seqüencia	[E.10]	1	0%	1%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	5	0%	0%	100%	0%	0%
	Manipulació de la configuració	[A.4]	5	85%	65%	90%	40%	75%
	Suplantació de la identitat de l'usuari	[A.5]	20	65%	25%	0%	50%	0%
	Aprofitament dels privilegis d'accés	[A.6]	5	5%	75%	0%	0%	0%
	Usos no previstos	[A.7]	35	0%	0%	65%	0%	0%
	[Re-]encaminament de missatges	[A.9]	5	50%	15%	0%	1%	1%
	Alteració de la seqüencia	[A.10]	5	0%	1%	0%	0%	0%
	Accessos no autoritzats	[A.11]	30	50%	35%	0%	50%	0%
	Repudi	[A.13]	5	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	8	0%	0%	100%	0%	0%
[S.6]	**Servei Web Marca [Z]**			**85%**	**75%**	**100%**	**50%**	**75%**
	Errors d'usuari	[E.1]	5	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	15	65%	75%	75%	50%	25%
	Errors de monitorització (log)	[E.3]	20	0%	0%	0%	0%	35%
	Errors de configuració	[E.4]	35	25%	40%	75%	50%	5%
	Errors de [re-]encaminament	[E.9]	1	1%	1%	0%	1%	1%
	Errors de seqüencia	[E.10]	1	0%	1%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	5	0%	0%	100%	0%	0%

	Manipulació de la configuració	[A.4]	5	85%	65%	90%	40%	75%
	Suplantació de la identitat de l'usuari	[A.5]	20	65%	25%	0%	50%	0%
	Aprofitament dels privilegis d'accés	[A.6]	5	5%	75%	0%	0%	0%
	Usos no previstos	[A.7]	35	0%	0%	65%	0%	0%
	[Re-]encaminament de missatges	[A.9]	5	50%	15%	0%	1%	1%
	Alteració de la seqüencia	[A.10]	5	0%	1%	0%	0%	0%
	Accessos no autoritzats	[A.11]	30	50%	35%	0%	50%	0%
	Repudi	[A.13]	5	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	8	0%	0%	100%	0%	0%
[S.7]	**Servei Web Promoció [2X]**			**85%**	**75%**	**100%**	**50%**	**75%**
	Errors d'usuari	[E.1]	5	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	15	65%	75%	75%	50%	25%
	Errors de monitorització (log)	[E.3]	20	0%	0%	0%	0%	35%
	Errors de configuració	[E.4]	35	25%	40%	75%	50%	5%
	Errors de [re-]encaminament	[E.9]	1	1%	1%	0%	1%	1%
	Errors de seqüencia	[E.10]	1	0%	1%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	5	0%	0%	100%	0%	0%
	Manipulació de la configuració	[A.4]	5	85%	65%	90%	40%	75%
	Suplantació de la identitat de l'usuari	[A.5]	20	65%	25%	0%	50%	0%
	Aprofitament dels privilegis d'accés	[A.6]	5	5%	75%	0%	0%	0%
	Usos no previstos	[A.7]	35	0%	0%	65%	0%	0%
	[Re-]encaminament de missatges	[A.9]	5	50%	15%	0%	1%	1%
	Alteració de la seqüencia	[A.10]	5	0%	1%	0%	0%	0%
	Accessos no autoritzats	[A.11]	30	50%	35%	0%	50%	0%
	Repudi	[A.13]	5	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	8	0%	0%	100%	0%	0%
[S.10]	**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%

[S.11]	**Servei Intercanvi de Fitxers**			**50%**	**25%**	**85%**	**50%**	**30%**
	Errors d'usuari	[E.1]	5	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	2	5%	1%	75%	5%	1%
	Errors de monitorització (log)	[E.3]	0	0%	0%	0%	0%	0%
	Errors de configuració	[E.4]	3	25%	5%	75%	15%	25%
	Errors de [re-]encaminament	[E.9]	10	25%	5%	0%	5%	5%
	Errors de seqüencia	[E.10]	0	0%	0%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	1	0%	0%	75%	0%	0%
	Manipulació de la configuració	[A.4]	1	50%	25%	50%	50%	25%
	Suplantació de la identitat de l'usuari	[A.5]	3	25%	25%	0%	50%	0%
	Aprofitament dels privilegis d'accés	[A.6]	0	0%	0%	0%	0%	0%
	Usos no previstos	[A.7]	5	0%	0%	85%	0%	0%
	[Re-]encaminament de missatges	[A.9]	3	40%	25%	0%	25%	30%
	Alteració de la seqüencia	[A.10]	1	0%	25%	0%	0%	0%
	Accessos no autoritzats	[A.11]	2	50%	25%	0%	45%	0%
	Repudi	[A.13]	1	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	2	0%	0%	75%	0%	0%
[S.12]	**Servei INFOLOG**			**50%**	**45%**	**50%**	**25%**	**25%**
	Errors d'usuari	[E.1]	75	0%	15%	1%	0%	0%
	Errors dels Administradors	[E.2]	3	1%	5%	1%	1%	1%
	Errors de monitorització (log)	[E.3]	10	0%	0%	0%	0%	25%
	Errors de configuració	[E.4]	1	5%	25%	5%	5%	5%
	Errors de [re-]encaminament	[E.9]	2	1%	25%	0%	5%	5%
	Errors de seqüencia	[E.10]	5	0%	45%	0%	0%	0%
	Parada del sistema per agotament dels recursos	[E.24]	1	0%	0%	45%	0%	0%
	Manipulació de la configuració	[A.4]	1	50%	45%	50%	25%	25%
	Suplantació de la identitat de l'usuari	[A.5]	10	1%	1%	0%	25%	0%
	Aprofitament dels privilegis d'accés	[A.6]	1	25%	5%	0%	0%	0%
	Usos no previstos	[A.7]	15	0%	0%	50%	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%	25%	0%	25%	0%
	Repudi	[A.13]	1	0%	0%	0%	0%	5%
	Denegació de servei	[A.24]	3	0%	0%	50%	0%	0%
[S.13]	**Servei SGANL**			**35%**	**50%**	**75%**	**15%**	**25%**
	Errors d'usuari	[E.1]	10	0%	15%	5%	0%	0%
	Errors dels Administradors	[E.2]	2	15%	25%	15%	5%	15%
	Errors de monitorització (log)	[E.3]	1	0%	0%	0%	0%	1%
	Errors de configuració	[E.4]	2	15%	25%	15%	1%	1%
	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%	25%	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]	3	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%
[S.16]	**Servei PRISMA**			**35%**	**50%**	**75%**	**15%**	**25%**
	Errors d'usuari	[E.1]	2	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	1	5%	5%	10%	5%	5%
	Errors de monitorització (log)	[E.3]	1	0%	0%	0%	0%	1%
	Errors de configuració	[E.4]	1	1%	5%	1%	1%	1%
	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%	25%	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%
[S.17]	**Servei ORALIMS**			**35%**	**65%**	**75%**	**15%**	**25%**
	Errors d'usuari	[E.1]	25	0%	65%	1%	0%	0%
	Errors dels Administradors	[E.2]	5	5%	5%	25%	5%	5%
	Errors de monitorització (log)	[E.3]	1	0%	0%	0%	0%	5%
	Errors de configuració	[E.4]	10	5%	50%	50%	1%	1%
	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%	45%	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%

[S.18]	**Servei CALOR**			**50%**	**50%**	**95%**	**25%**	**25%**
	Errors d'usuari	[E.1]	25	0%	5%	1%	0%	0%
	Errors dels Administradors	[E.2]	3	15%	25%	25%	5%	5%
	Errors de monitorització (log)	[E.3]	5	0%	0%	0%	0%	25%
	Errors de configuració	[E.4]	2	5%	5%	15%	25%	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]	10	0%	0%	95%	0%	0%
	Manipulació de la configuració	[A.4]	1	50%	50%	50%	25%	15%
	Suplantació de la identitat de l'usuari	[A.5]	3	25%	25%	0%	25%	0%
	Aprofitament dels privilegis d'accés	[A.6]	1	25%	25%	0%	0%	0%
	Usos no previstos	[A.7]	5	0%	0%	85%	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]	3	15%	15%	0%	25%	0%
	Repudi	[A.13]	1	0%	0%	0%	0%	25%
	Denegació de servei	[A.24]	1	0%	0%	85%	0%	0%
[S.20]	**Servei FileServer ES**			**50%**	**30%**	**85%**	**35%**	**25%**
	Errors d'usuari	[E.1]	75	0%	30%	1%	0%	0%
	Errors dels Administradors	[E.2]	3	50%	25%	30%	5%	5%
	Errors de monitorització (log)	[E.3]	0	0%	0%	0%	0%	0%
	Errors de configuració	[E.4]	5	15%	15%	15%	15%	15%
	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]	4	0%	0%	85%	0%	0%
	Manipulació de la configuració	[A.4]	1	50%	25%	50%	35%	25%
	Suplantació de la identitat de l'usuari	[A.5]	5	25%	25%	0%	25%	0%
	Aprofitament dels privilegis d'accés	[A.6]	3	25%	25%	0%	0%	0%
	Usos no previstos	[A.7]	5	0%	0%	35%	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	15%	15%	0%	25%	0%
	Repudi	[A.13]	1	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	1	0%	0%	75%	0%	0%
[S.21]	**Servei FileServer PT**			**50%**	**30%**	**85%**	**35%**	**25%**
	Errors d'usuari	[E.1]	75	0%	30%	1%	0%	0%
	Errors dels Administradors	[E.2]	3	50%	25%	30%	5%	5%
	Errors de monitorització (log)	[E.3]	0	0%	0%	0%	0%	0%
	Errors de configuració	[E.4]	5	15%	15%	15%	15%	15%
	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]	4	0%	0%	85%	0%	0%

	Manipulació de la configuració	[A.4]	1	50%	25%	50%	35%	25%
	Suplantació de la identitat de l'usuari	[A.5]	5	25%	25%	0%	25%	0%
	Aprofitament dels privilegis d'accés	[A.6]	3	25%	25%	0%	0%	0%
	Usos no previstos	[A.7]	5	0%	0%	35%	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	15%	15%	0%	25%	0%
	Repudi	[A.13]	1	0%	0%	0%	0%	1%
	Denegació de servei	[A.24]	1	0%	0%	75%	0%	0%

3.7.- Impacte Potencial

Donat que hem classificats els actius en uns rangs al qual li hem atorgat un valor referencia en cada dimensió de seguretat, i atès que coneixem les amenaces amb el seu impacte de degradació que suposen per aquestes dimensions, estem en disposició de poder calcular l'impacte potencial que pot suposar per a l'empresa la materialització de les amenaces. Aquest càlcul (sense tenir en compte cap contramesures, ja que encara no hem parlat de les que ja es trobem instal·lades a l'organització) es permetrà obtenir un valor referencia que permetrà prioritzar el pla d'acció, i alhora, avaluar com es veu modificat aquest valor un com s'apliquin contramesures (implantades ja o possibles projectes futurs).

Per tal de poder obtenir aquest valor; farem servir la següent formula per obtenir aquest impacte potencial:

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

Cal destacar en aquest punt; que tant el valor de l'impacte que imputarem sobre cada actiu, serà el màxim dels impactes de les amenaces que es podem materialitzar sobre cada actiu. Principalment apliquem aquest criteri ja que normalment a l'hora d'incorporar contramesures l'ordre a seguir serà de les que redueixin en major mesura el valor de l'impacte a les que redueixin en menor valor aquest paràmetre.

Per tant un cop aclarit aquest concepte, observem que l'impacte potencial sobre els nostres actius serà:

ACTIU		Valoració					IMPACTE					IMPACTE POTENCIAL				
		C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[S.1]	Servei de Correu Usuaris	8	7	8	6	6	**85%**	**75%**	**100%**	**65%**	**85%**	6,80	5,25	8,00	3,90	5,10
[S.3]	Servei Intranet	8	8	6	9	7	75%	75%	100%	50%	35%	6,00	6,00	6,00	4,50	2,45
[S.4]	Servei Web Marca [X]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
[S.5]	Servei Web Marca [Y]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
[S.6]	Servei Web Marca [Z]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
[S.7]	Servei Web Promoció [2X]	6	7	5	4	4	85%	75%	100%	50%	75%	5,10	5,25	5,00	2,00	3,00
[S.10]	Servei SKEP	5	9	7	7	5	35%	50%	85%	15%	25%	1,75	4,50	5,95	1,05	1,25
[S.11]	Servei Intercanvi de Fitxers	3	3	4	2	2	50%	25%	85%	50%	30%	1,50	0,75	3,40	1,00	0,60

[S.12]	Servei INFOLOG	5	8	10	7	5	50%	45%	50%	25%	25%	2,50	3,60	5,00	1,75	1,25
[S.13]	Servei SGANL	5	7	8	5	5	35%	50%	75%	15%	25%	1,75	3,50	6,00	0,75	1,25
[S.16]	Servei PRISMA	3	7	4	3	3	35%	50%	75%	15%	25%	1,05	3,50	3,00	0,45	0,75
[S.17]	Servei ORALIMS	7	9	8	9	9	35%	65%	75%	15%	25%	2,45	5,85	6,00	1,35	2,25
[S.18]	Servei CALOR	6	8	10	8	8	50%	50%	95%	25%	25%	3,00	4,00	9,50	2,00	2,00
[S.20]	Servei FileServer ES	6	8	7	4	4	50%	30%	85%	35%	25%	3,00	2,40	5,95	1,40	1,00
[S.21]	Servei FileServer PT	6	8	7	4	4	50%	30%	85%	35%	25%	3,00	2,40	5,95	1,40	1,00

3.8.- Resum Objectius aconseguits

Tal com hem pogut observar a les taules dels apartats 3.5, 3.6 i 3.7 d'aquest apartat; completades a la informació corresponent als actius presents que hi ha sobre la nostra organització, disposem de:

- Una anàlisi detallada dels actius rellevants a nivell de seguretat per a l'organització.
- 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 que estan exposades els nostres actius (sense contar cap contra mesura de les instal·lades).

En aquest punt, cal destacar però que el risc no serà en general eliminable (per exemple, probablement no podrem aïllar la nostra empresa o fer immune als desastres naturals), però sí gestionable. Per tant, l'aplicació de les mesures de seguretat existents (con possibles projectes futurs), milloraran la gestió d'aquest riscos.

4.- AUDITORIA DE COMPLIMENT DE LA ISO:IEC 27002:2005

4.1.- Introducció

Ara que coneixem els actius de l'empresa i hem avaluat les amenaces; és el moment d'avaluar fins a quin punt l'empresa compleix amb les bones pràctiques en matèria de seguretat. La ISO27002:2005 ens servirà com a marc de control de l'estat de la seguretat. Conjuntament amb l'anàlisi de riscos realitzat, ens permetrà plantejar un conjunt de projectes per a la millora de la seguretat en l'organització. Serà la base del futur pla d'acció a implementar d'aquest pla director.

4.2.- Metodologia a utilitzar

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.

4.3.- Avaluació de la maduresa

L'objectiu d'aquest apartat del PDS és avaluar la maduresa de la seguretat pel que fa ales diferents dominis de control i els 133 controls plantejats per la ISO / IEC 27002:2005. Abans d'abordar intentarem aprofundir al màxim en el coneixement de l'organització.

De forma resumida, els dominis que s'han d'analitzar són:

- Política de seguretat.
- Organització de la seguretat de la informació.
- Gestió d'actius.
- Seguretat en els recursos humans.

- Seguretat física i ambiental
- Gestió de comunicacions i operacions.
- Control d'accés.
- Adquisició, desenvolupament i manteniment de Sistemes d'Informació.
- Gestió d'incidents
- Gestió de continuïtat de negoci
- Compliment

L'estudi farà una revisió dels 133 controls plantejats per la norma per complir amb els diferents objectius de control – el nombre dels quals pot ser donada per a cada un dels dominis-. Aquesta estimació la farem segons la següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM):

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.

4.4.- Presentació de resultats

4.4.1.- Resultats per Domini

En aquest apartat podrem veure els resultats obtinguts al realitzar l'anàlisi de tots els controls dels diferents dominis de la reglamentació ISO, en funció de la valoració dels resultats observats, aplicant el criteri de maduresa definit en l'apartat anterior:

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%
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%
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%

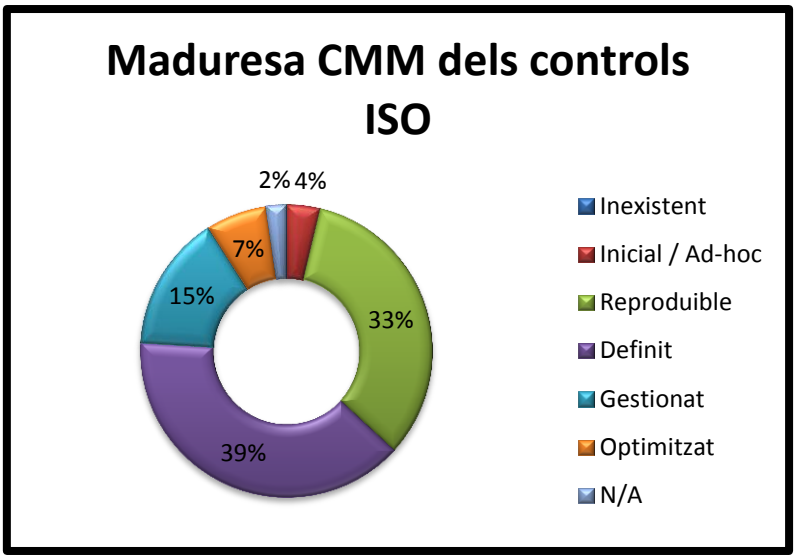
10.7.4 Seguretat de la documentació del sistema	55%
10.8 Intercanvi de informació	**59%**
10.8.1 Política i procediment de intercanvi de informació	60%
10.8.2 Acord de intercanvi	40%
10.8.3 Suport físic en transit	35%
10.8.4 Missatgeria electrònica	75%
10.8.5 Sistemes de informació empresarials	85%
10.9 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%
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%
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%
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%

4.4.2.- Resultats en funció de la Maduresa

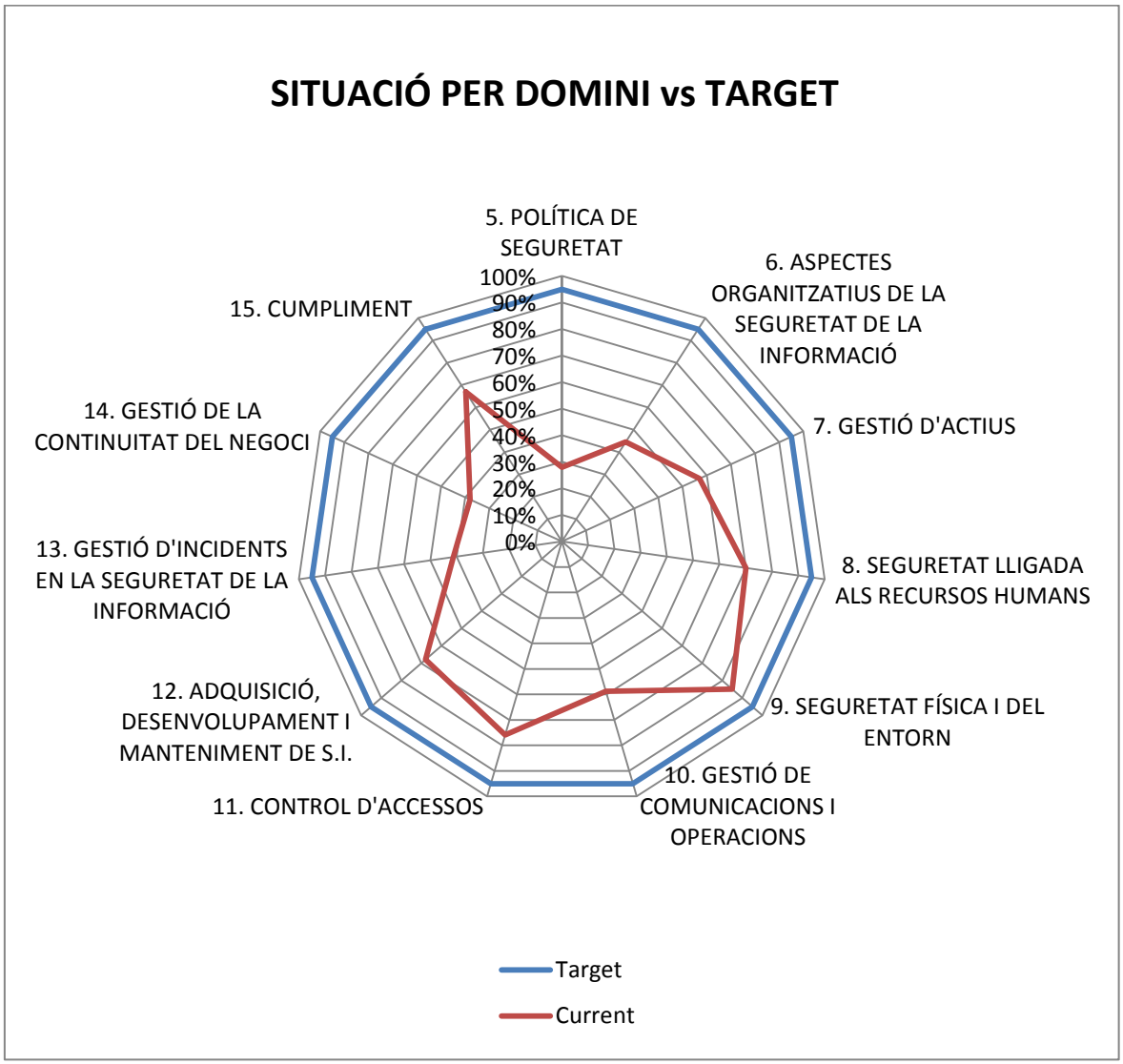
Com a resultat sintètics, és interessant avaluar el nivell de maduresa percentual dels diferents controls. És a dir, per als 133 controls, quin grau de maduresa té cada un, cosa que ens dóna una visió de l'estat de la seguretat en conjunt:



4.4.3.- Resultats respecte el Target definit i observacions per Domini

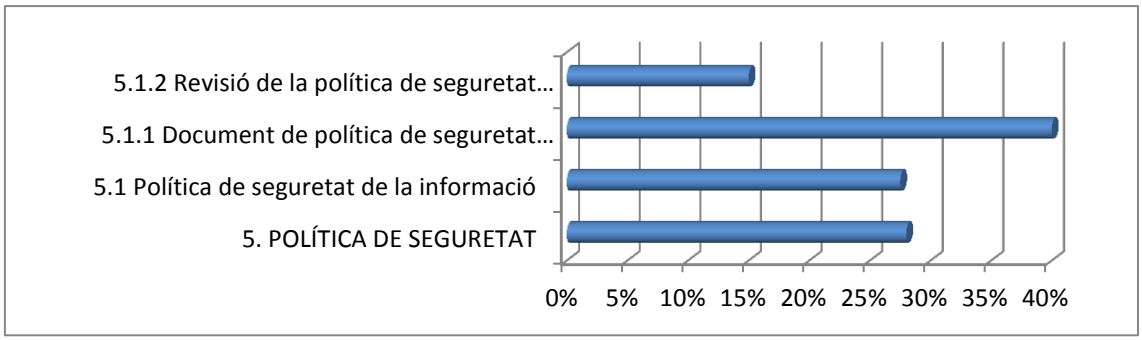
De cara a poder establir els objectius al qual vol arribar la nostra empresa en cada domini, i tot i ser-hi una empresa privada que a priori no tindria cap obligació a arribar a un nivell mínim ja que no requereix per cap obligació l'obtenció de la certificació; s'ha decidit des de la direcció donar una certa rellevància a la qualitat dels controls de seguretat i es vol arribar a obtenir un nivell de resultat **del 95% en tots els dominis** a la finalització d'aquest pla director (pròxims 4 anys) de cara a obtenir els beneficis que s'obtenen amb la maduresa del model presentat a l'ISO i a la vegada estar en disposició de sol·licitar la certificació en cas necessari.

Mitjançant la representació del resultat utilitzant un "diagrama de radar" podem observar una visió més detallada del nivell de compliment per capítol ISO. Anticipant-nos a les mesures o futurs projectes, serà interessant comparar l'estat actual de cada domini amb l'estat desitjat:



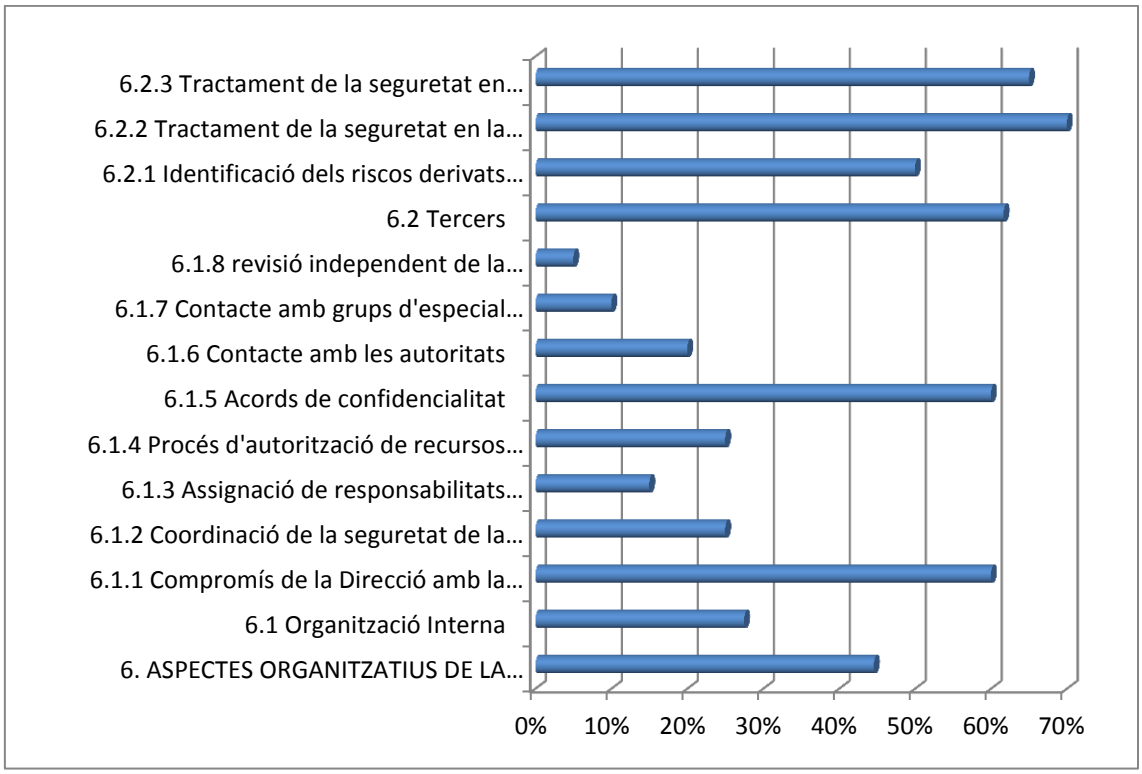
A la seva vegada i un cop analitzat el resultat global, resulta interessant analitzar gràficament cada Domini establert amb detall, ja que el resultat obtingut pot ser degut a una deficiència particular d'un dels Objectius de control que el formen o pot ser una deficiència molt plausible en un (o varis) controls del domini. Per tant i analitzar per dominis, el resultat observat, quedaria de la següent forma:

POLÍTICA DE SEGURETAT



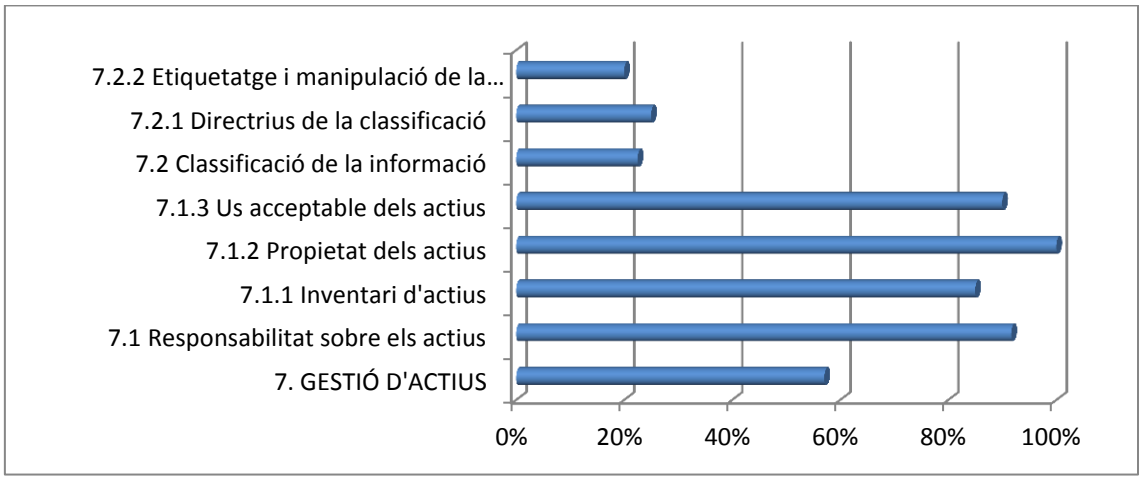
Com podem veure, en aquest domini concret, els objectius principals que s'hauran de buscar en el projectes o procediments futurs amb d'anar enfocats a la millora del document que fa referencia a la política de seguretat, i a la seva vegada a la posada en marxa d'un cicle de revisió sobre aquest document (seguint el model del cicle de Deming ja comentat) per tal d'evolucionar i actualitzar el document perquè sigui òptim a la situació present de l'empresa en tot moment.

ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ



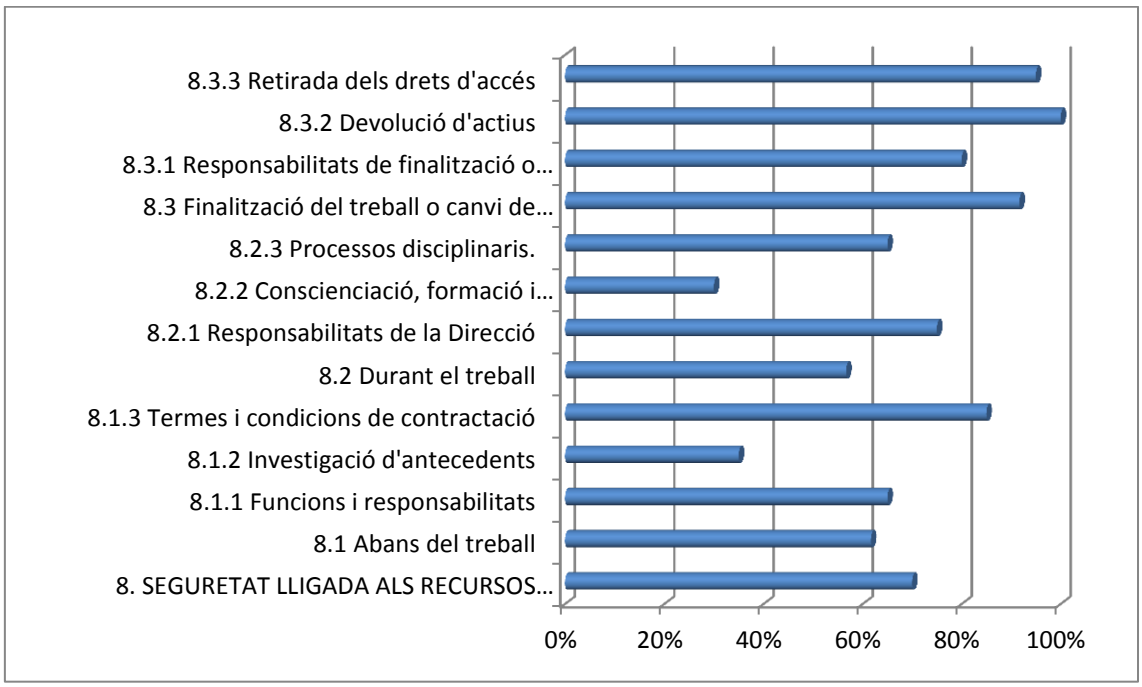
Aquest domini, veiem clarament que la seva valoració global s'ha vist molt penalitzada degut principalment a una falta d'organització interna en els seus diferents punts i en menor mesura s'hauran de polir certs aspectes en relació a la identificació de riscos i tractament de la seguretat en els casos en relació a les empreses externes amb les que es treballa.

GESTIÓ D'ACTIUS



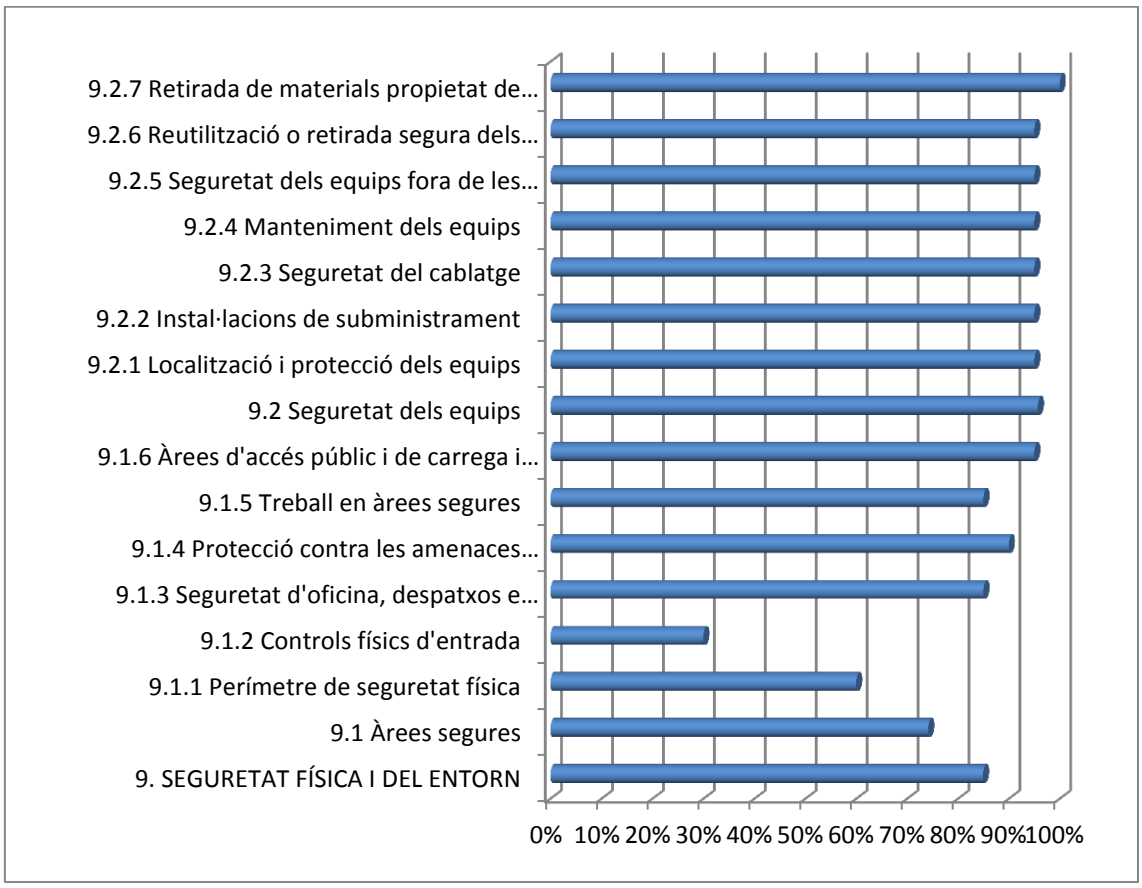
Veiem que aquest domini es troba molt a prop del seu valor objectiu, ja que la seva penalització es troba focalitzada en el fet que la informació no ha estat tractada com un actiu. Per tant l'objectiu futur serà implementar els procediments per realitzar aquest tractament.

SEGURETAT LLIGADA ALS RECURSOS HUMANS



En aquest domini, a nivell global podem observar ràpidament que te controls molt a prop del objectiu fitxat per la seva valoració però cal aprofundir en certs controls específics com son la investigació d'antecedents i la conscienciació, formació interna i depurar alguns punts sobre la resta de controls de cara a complir els objectius. Cal dir que en aquest domini concret, la consecució de l'objectiu no requereix canvis concrets a implementar però si tenir clar els diferents controls i com afrontar-los. Podríem dir que per aquest domini, es tractarà més d'una organització dels procediments d'actuació a realitzar que la implantació d'un projecte concret.

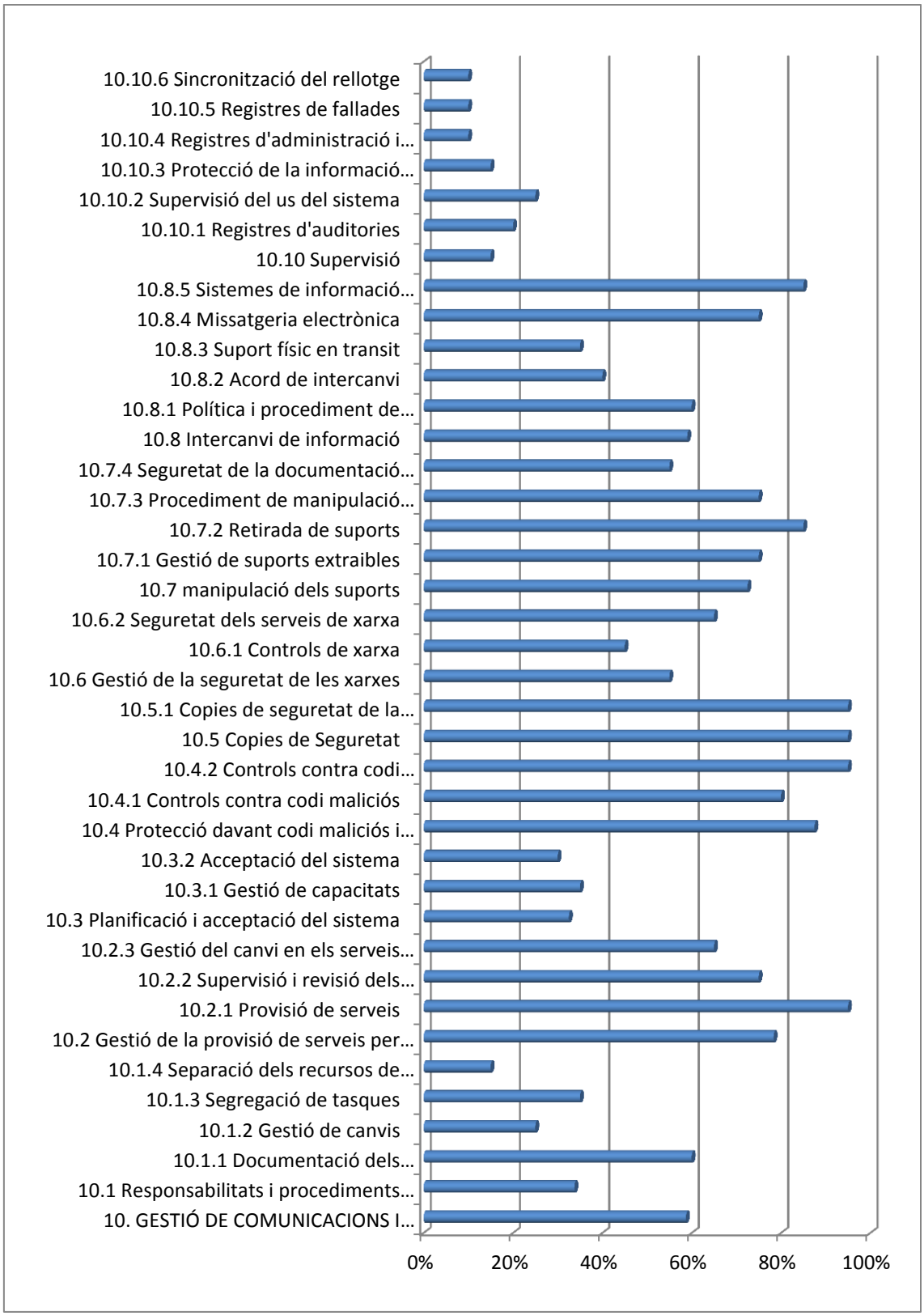
SEGURETAT FÍSICA I DEL ENTORN



Com podem veure molt clarament, aquest es un dels dominis que es troba molt a prop de la consecució de l'objectiu global i la pèrdua de la valoració es troba concretament en la delimitació del perímetre de treball amb les àrees segures i la identificació dels controls físics d'entrada que ha estat un punt que fins ara no s'ha donat molta importància i amb el volum de treballadors actuals i el nombre de visites, personal extern, proveïdors. Etc. Cal començar a avaluar.

Focalitzarem els nostres esforços a identificar ràpidament les mesures a implementar per solventar ràpidament aquest punt concrets, i els detall concrets que podem faltar a la resta de punts

GESTIÓ DE COMUNICACIONS I OPERACIONS

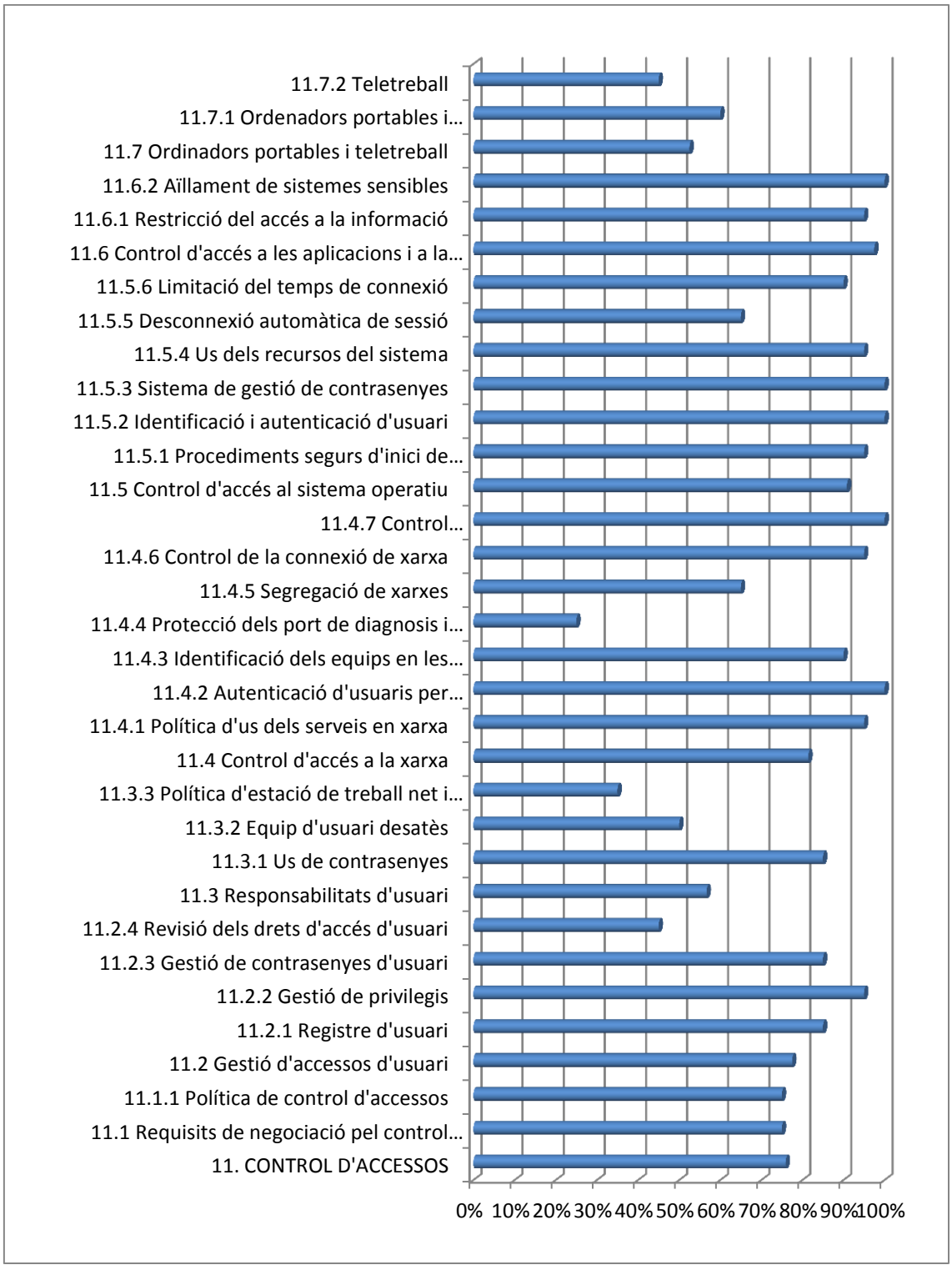


Com podem observar visualment aquest domini presenta moltes àrees d'actuació, d'entre les que caldria destacar que inicialment haurem de focalitzar els nostres esforços en totes les tasques i funcions que s'encarreguen principalment de la supervisió, ja que degut a la falta de

recursos del passat aquestes tasques havien estat molt reduïdes o inclús eliminades en alguns punts concrets de l'àrea de sistemes de la informació. A nivell de planificació en la gestió de les comunicacions, com en la definició de procediments d'actuació i responsabilitats, veiem també uns valors molt inferiors a la resta de controls, donat al mateix factor que la supervisió; davant la falta de recursos, es va prendre la decisió de reduir dràsticament totes les parts que no afecten directament sobre les comunicacions i les operacions. Aquesta reducció de recursos també va impactar en altres controls dels que marca l'ISO reduint la seva valoració actual.

Com s'ha comentat en el paràgraf anterior, donada la reducció de recursos assignats a aquest domini dintre de l'organització en el passat, ens trobem avui dia amb un domini molt focalitzat a oferir el seu objectiu amb els mínims recursos, i per tant podríem dir que la comunicació i les operacions estan garantides de forma mínima però la gestió de les mateixes ha sofert una gran reducció en la seva qualitat. L'objectiu futur, ha de passar clarament per destinar els recursos necessaris tant pels projectes a implementar com pels recursos per establir els diferents procediments o les pròpies tasques de supervisió i poder tornar a establir aquest model dintre d'una metodologia d'aprenentatge i evolució.

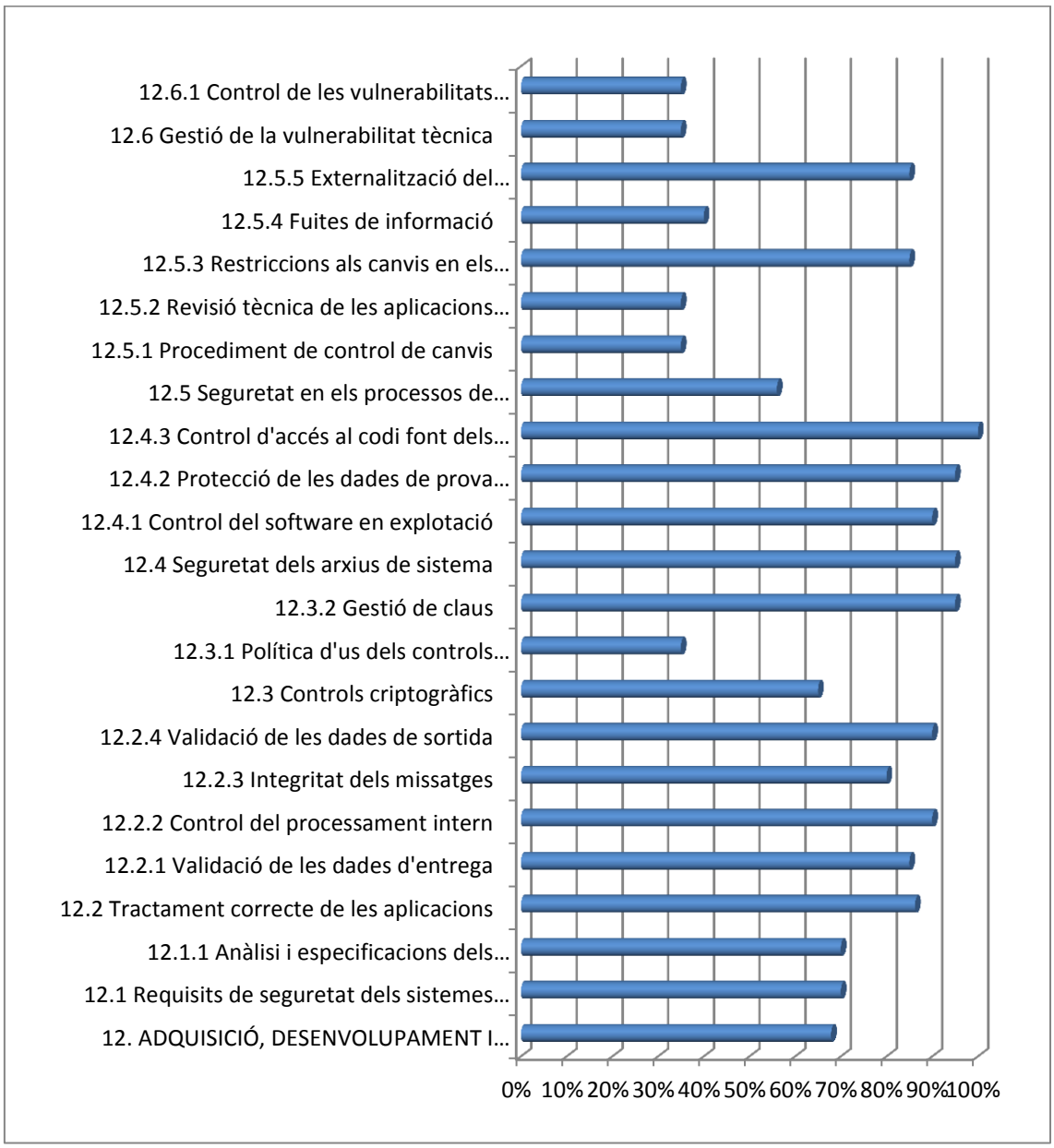
CONTROL D'ACCESSOS



Tot i la disparitat de valoracions en els controls d'aquest domini, veiem que els punts que haurem d'atacar clarament en el futur seran principalment tota la part relacionada amb els control d'accessos relativa al teletreball com les responsabilitats dels usuaris sobre els seus accessos. A nivell puntual veiem que certs controls necessitaran certes millors per acabar

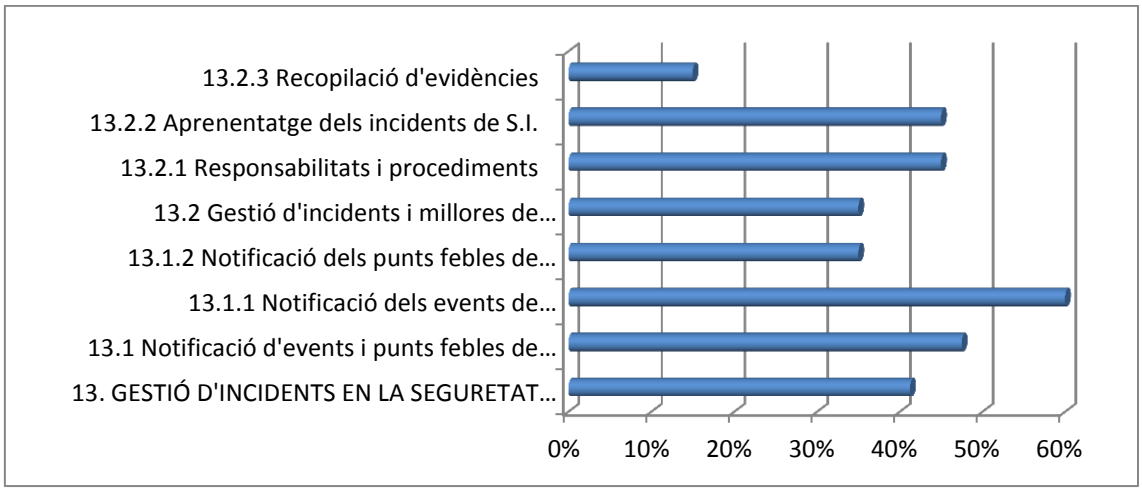
d'obtenir la valoració objectiu mitjançant l'establiment dels diferents procediments (principalment) de cara a millorar la seva valoració puntual. Un exemple d'això seria la protecció dels port de diagnosis i control o la pròpia revisió dels drets d'accés. Com veiem de cara a millorar aquests punts, establirem procediments d'actuació a complir tant pel personal de sistemes com dels propis usuaris que al cap i la fi han de prendre consciencia de les seves obligacions respecte als accessos dels quals disposen.

ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMIENT DELS SISTEMES DE INFORMACIÓ



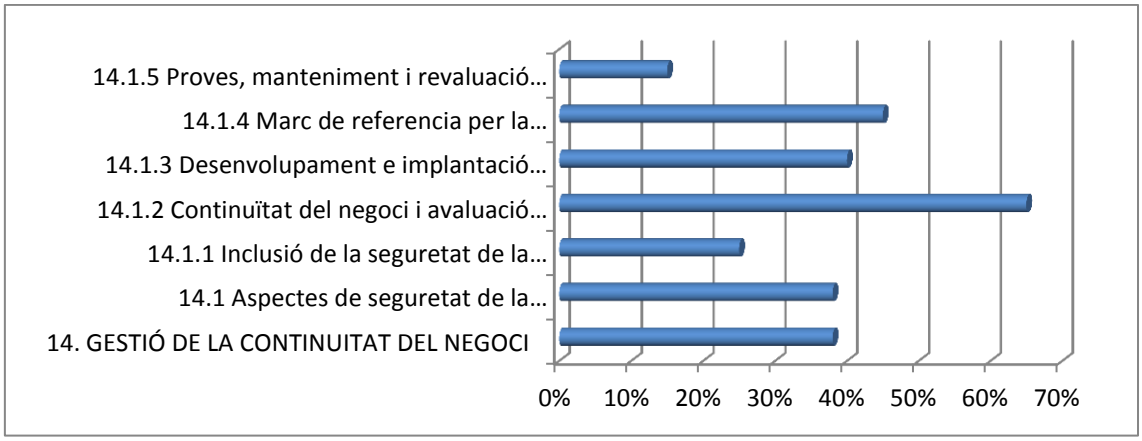
En aquest domini la millora de la seva valoració passa principalment per l'establiment d'una metodologia de treball a seguir amb els S.I. i que s'encarregui d'establir els procediments o mecanismes necessaris per tal de garantir els diferents controls que podem observar que no arriben a complir l'objectiu fitxar pel comitè de Seguretat i respatllat pel comitè de direcció.

GESTIÓ D'INCIDENTS EN LA SEGURETAT DE LA INFORMACIÓ



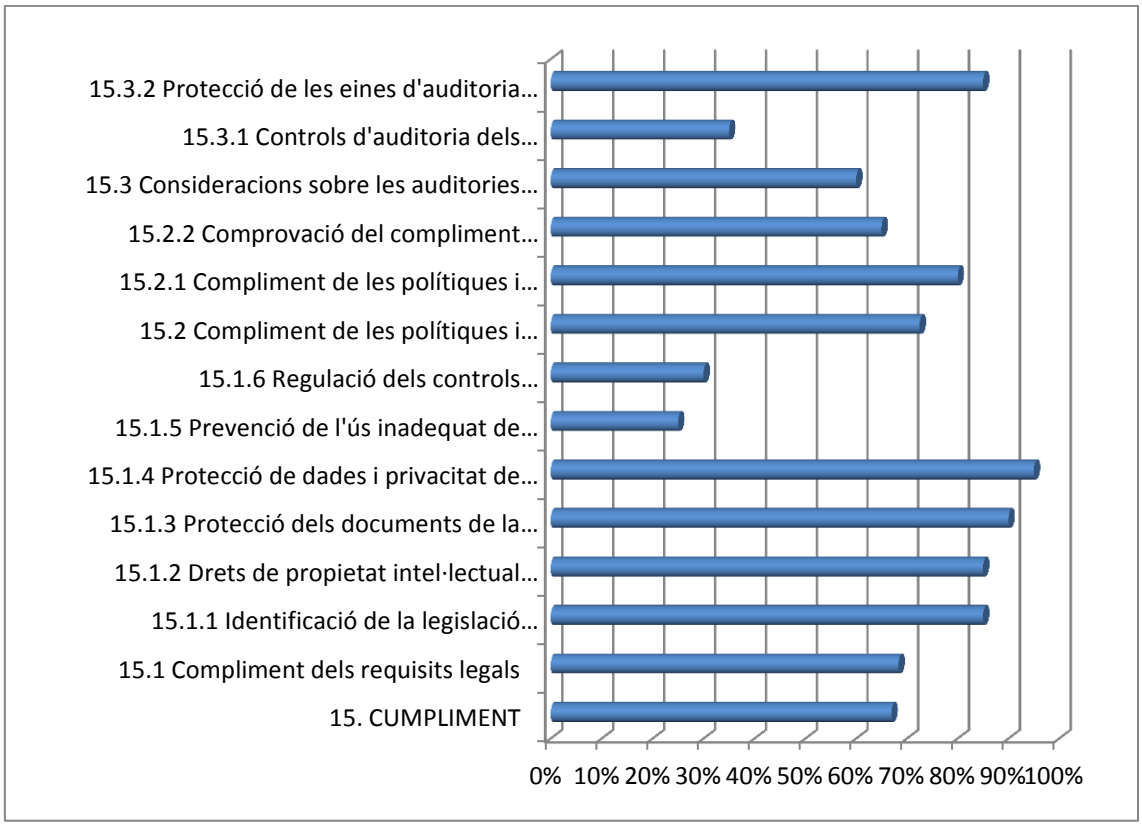
Aquest domini es focalitza sobre la gestió d'incidents en la seguretat de la informació, i podem observar clarament que tant la notificació com la gestió i millora per tracta aquest tipus d'esdeveniments cal millorar-lo per tal d'arribar a l'objectiu fitxat. En aquest cas ens focalitzarem en dues línies de treball, d'una banda com afrontar l'incident des de el moment inicial o de detecció fins a la resolució del mateix, i d'altra banda, com aprofitar el treball realitzat en la resolució de cara a futures situacions, es a dir, aprendre de les diferents situacions i millorar la nostra gestió.

GESTIÓ DE LA CONTINUITAT DEL NEGOCI



Aquest domini es troba molt penalitzat pel fet que la continuïtat del negoci no esta tractada des d'un punt global dintre de l'organització, sinó que ha estat plantejada de forma molt puntual i sense coordinació dintre d'algunes àrees solament. Haurem d'establir un equip de treball focalitzat en la continuïtat del negoci, per tal d'analitzar la situació actual, els possibles riscos i plantejar els diferents escenaris de resolució de cara a poder tenir clar com hem de reaccionar en cas necessari. Veiem clarament, que es tracta d'un treball d'anàlisi i decisió respecte a les possibles situacions adverses pel negoci.

COMPLIMENT



En aquest domini, veiem clarament que d'entrada haurem de focalitzar els nostres esforços tant en la regulació dels controls com en la prevenció dels usos inadequats que veiem que son els dos punts més febles del domini donat que no s'han tractat amb molt interès en el passat ni s'han destinat els recursos necessaris; com el propi control sobre les auditories dels sistemes de la informació. Un cop abordats aquest tres punt dèbils, plantejarem els diferents procediments de cara a obtenir el valor desitjat per la resta de controls.

4.5.- Conclusions

Com hem pogut veure en el desenvolupament d'aquest mòdul; hem pogut conèixer tant quantitativament com gràficament la valoració pels diferents capítols de la ISO/IEC27002:2005 i del seu compliment i en aquest moment tenim una visió molt clara de quina es la situació actual de la nostra organització en aquest àmbit. Per tant, i donat que ja hem presentat l'objectiu de compliment que es vol assolir a l'organització i a la incorporació de la informació provinent del anàlisi de riscos; estem en plena disposició de plantejar el pla d'acció pels pròxims 4 anys d'aquest pla director en matèria de seguretat.

Dintre de l'anàlisi per domini que hem realitzat, hem pogut observar on es trobem les majors mancances de la nostra organització i amb la incorporació de les dades de l'anàlisi de riscos, podrem confeccionar detalladament un pla d'acció per a presentar a la direcció de l'organització i poder validar la seva viabilitat dintre del context actual en el que es troba l'organització i el seu volum de producció. Evidentment, aquest pla es confeccionarà a partir de les premisses indicades per la direcció de l'organització, mitjançant les quals a recolzat plenament la necessitat de la confecció d'aquest PDS i la seva voluntat d'analitzar, estudiar i disponibilitat els recursos necessaris per arribar a tal objectiu.

En observat a cada domini, quin serà els punts sobre els quals caldrà focalitzar els nostres esforços i aquesta valoració, ens servirà com eina de mesura dintre dels pròxims 4 anys valorant com evolucionem en cadascun dels capítols/àmbits als que fa referència l'ISO i que al cap i a la fi, juntament amb l'anàlisi de riscos, busquem l'objectiu de controlar i gestionar la seguretat dels sistemes de la informació en la nostre organització i estar preparats per tot tipus de situacions que es podem dar dintre d'aquesta matèria. Per tant veiem clarament que el futur es presenta com un procés de millora continua sobre els diferents dominis que indica l'ISO i en el qual l'objectiu comú serà l'obtenció del nivell desitjat per tal contar clarament amb indicadors numèrics i estadístics per seguir l'evolució dels diferents processos involucrats com disposar de tecnologia per automatitzar el flux de treball, amb l'ús d'eines per millorar la qualitat i l'eficiència, i en definitiva aproximar-nos a l'excel·lència operacional en matèria de seguretat de la informació dintre de la nostra organització.

5.- PROPOSTES DE MILLORES

En aquest punt d'aquest PDS, estem en disposició gracies a l'anàlisi de riscos i l'estudi del nivell de compliment dels controls ISO, de poder conèixer amb molta exactitud l'estat de la seguretat de la nostra empresa i es el moment de plantejar les diferents iniciatives, millores o projectes per tal de millorar l'estat de la seguretat en la nostra organització i anar poc a poc apropant-nos als nostres objectius finals, com som la reducció i control del risc e impacte al qual l'organització esta esposada i anar evolucionant cap a un nivell de maduresa optimitzat a nivell de compliment dels diferents dominis indicats per l'ISO.

Per tant en aquest capítol del PDS; ens centrarem en l'anàlisi i estudi de les diferents iniciatives a **plantejar e implementar en el pròxims 4 anys** que dura aquest PDS per tal d'arribar als objectius fixats des de la pròpia direcció de l'organització.

5.1.- Llistat de millores / Projectes

De cara a complir els objectius marcats per la direcció de l'organització, passem a detallar la relació d'iniciatives i projectes a implementar durant el període d'aquest PDS mitjançant una nomenclatura organitzada i estandarditzada que ens permeti a posteriori realitzar els resums gràfics per una ràpida assimilació dels diferents escenaris i situacions que es donaran durant els diferents terminis (curt, mitjà i llarg) d'implementació d'aquest PDS.

En cada un dels nostres projectes podrem veure clarament com reacciona el risc o l'impacte sobre l'organització, l'evolució respecte el nivell de compliment respecte els controls de l'ISO, els beneficis aportats **a tota l'organització** (no solament a l'àrea de sistemes de la informació); la previsió econòmica de la implementació i per últim la planificació temporal tant necessària per implementar-lo com la pròpia planificació respecte la resta de projectes que l'organització ha de desenvolupar. En aquest apartat, veurem les necessitats pròpies del projecte, i a l'apartat següent veurem com queda el conjunt de projectes planificats en el termini establert per aquest PDS.

Per tant els projectes/iniciatives que considerem cal implementar a la nostra organització seran:

Nom: **"VIRTUALITZACIÓ PLENA"**
Referència: **PRO/TEC - 001**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: Es tracta d'un projecte purament tècnic on el seu objectiu principal es reduir al màxim la possibilitat de indisponibilitat dels serveis utilitzats a l'organització per fallades físiques del propi hardware utilitzat. A la seva vegada s'elevarà la disponibilitats de tots els serveis a un valor del 99% anual.
Com objectiu secundari, es realitzarà una re agrupació de serveis comuns utilitzats de cara a organitzar un millor servei de manteniment des del departament de S.I. de l'organització agrupant entre d'altres totes les bases de dades sobre un mateix SGBD i gestionant una solució complerta de seguretat de la informació per aquestes dades.

Descripció: L'objectiu final es utilitzar una plataforma virtualitzada (com la ja utilitzada a la part de la intranet de l'organització) per tal de gestionar tots els serveis tècnics ofertats directament als usuaris finals o necessaris pels diferents sistemes de l'organització, per tant serà necessari realitzar un estudi de les necessitats actuals dels diferents sistemes, una previsió de requeriments pels pròxims 4 anys (període comptable d'amortització d'una solució hardware com la que estem plantejant) i analitzar la possibilitat de realitzar-ho juntament amb la part existent que dona servei a la intranet corporativa (economia d'escala per obtenir unes despeses menors).

BENEFICIS

Pel departament S.I.:

- Reducció al mínim de la possibilitat de fallada hardware.
- Reducció al mínim del temps de indisponibilitat dels serveis, muntatge i manteniment.
- Reducció en el temps de posada en marxa d'un nou servei.
- Independència total del Sistema, la infraestructura necessària i les dades del sistema.
- Reducció elevada del temps de recuperació en cas de desastre.
- Estandardització de la solució hardware utilitzada, i per tant, major experiència pel personal del departament.
- Reducció tant del cost d'arrancada de servei (CAPEX) com del cost de manteniment del servei (OPEX).

Per l'organització:

- Reducció del temps de posada en marxa d'un nou servei.
- Major temps de disponibilitat dels serveis.

COST	
Temporal:	**Econòmic:**
3 mesos	200 K€

Nom: "Organització Servei intercanvi de dades (FTP Secure)"
Referència: PRO/TEC - 002
Requeriments / Predecessors:

- PRO/TEC – 001 (per aprofitar els beneficis del projecte anterior)

Objectiu: Aquest projecte purament tècnic persegueix l'objectiu d'estandarditzar un únic model d'intercanvi d'informació entre els sistemes i també amb l'exterior en cas necessari; amb la gestió del seguretat corresponent dintre del sistema, permetent tenir el control sobre tots els intercanvis i conèixer en tot moment qui i com esta realitzant els accessos a la informació aquí allotjada.

Descripció: Totes les solucions actuals per compartir informació entre sistemes i amb l'exterior passaran a utilitzar una solució única que s'encarregarà de gestionar els accessos i controlar el servei en tot moment per oferir el millor servei amb el rigor de complir les premisses de seguretat indicada per cada tipus de informació en funció de la seva classificació interna dintre de l'organització.

BENEFICIS

Pel departament S.I.:

- Utilització d'una plataforma comú per tots els intercanvis.
  - Major coneixement de la solució pel personal.
- Control total sobre els accessos i la informació intercanviada.
- Agrupació dels diferents serveis actuals en 1 sol servei.
- Possibilitat d'oferir la traçabilitat de la informació.
- Beneficis aportats per PRO/TEC – 001 a nivell de disponibilitat i fallida hardware.

Per l'organització:

- Model únic gestionat per aquest servei.
- Major seguretat en el tractament de la informació.
- Disponibilitat de la traçabilitat de la informació.

COST	
Temporal:	**Econòmic:**
20 dies	2,5K€

Nom: "Seguretat perimetral Xarxa (Firewall + IDS)"
Referència: PRO/TEC - 003
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: Actualitzar la solució actual software utilitzada per gestionar la seguretat perimetral que es troba obsoleta i no permet realitzar un servei òptim per les necessitats actuals e implementar una solució hardware dedicada que doni un mayor servei i rendiment.
Descripció: Donada la situació obsoleta i amortitzada del ISA Server 2006 utilitzat a l'organització per garantir la seguretat perimetral de la xarxa, es vol implementar una solució hardware dedicada exclusivament per aquesta tasca, i que incorpori els serveis de traçabilitat i detecció d'atacs de cara a poder millorar la seguretat tant en atacs des de l'exterior com poder controlar els atacs interns (servei actualment no possible) i la pròpia monitorització de tot el tràfic de l'organització.

BENEFICIS

Pel departament S.I.:

- Servei actualitzat a les tècniques actuals d'atacs.
- Nou servei de detecció d'intrusions.
- Monitorització del tràfic complert de la xarxa.
- Gestió dels serveis oferts entre les diferents xarxes corporatives utilitzades.
- Funcionalitats noves per evitar els atacs interns.
- Control total del tràfic de xarxa i possibilitat de estudiar l'historial de tràfic de l'organització amb major nivell de detall.
- Millor gestió dels accessos des de l'exterior.

Per l'organització:

- Major seguretat respecte els atacs informàtics.

COST	
Temporal: 20 dies	**Econòmic:** 13,5K€

Nom: **"Creació pla de continuïtat de negoci (BCP)"**
Referència: **INI/DOC - 001**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: De cara a poder gestionar una situació futura de materialització de qualsevol desastre que pugui afectar a l'organització cal dissenyar un pla complert per l'organització de cara a estar preparats davant d'una situació adversa d'aquest tipus que pugui afectar als sistemes de l'organització. Per tal de estar preparats, es realitzarà un seguiment continu realitzat per un comitè de seguretat que es definirà per part de l'organització i les diferents formacions o proves de nivell per evolucionar el pla creat per arribar a un nivell òptim que permeti fer front amb les millors condicions possibles dintre dels medis que disposa l'organització.

Descripció: A partir de l'anàlisi de riscos realitzats, i amb la creació d'un comitè de seguretat, s'encarregaran de la creació d'un pla per garantir la continuïtat del negoci amb el seu posterior seguiment i preparació/proves de totes les parts integrants d'aquest pla. Un cop conegut el risc assumit per l'organització i fixat dintre del nivell acceptat per la direcció, es definirà un pla anual d'evolució continuada i manteniment d'aquest BCP. Aquest pla serà revisat completament cada dos anys i entre aquestes revisions serà mantingut i coordinat pel equip de seguretat de l'organització.

BENEFICIS

Pel departament S.I.:

- Creació, evolució i prova dels plans de recuperació per a cada sistema.
- Gestió del risc i control de les diferents situacions que poden afectar als sistemes.
- Preparació davant de les adversitats.
- Budget específic assignat anualment per la realització d'aquestes activitats amb el suport de la direcció de l'organització.
- Personal preparat per reaccionar davant les adversitats per tal d'aconseguir un menor temps d'afectació i minimitzar l'impacte sobre l'organització.

Per l'organització:

- Anticipació davant una situació adversa que afecti al negoci.
- Formació i organització davant de qualsevol adversitat.
- Risc al que estem exposats conegut, controlat i gestionat.
- Garantir una ràpida resolució i tornada a la situació estable de les activitats considerades con fonamentals (core) del nostre negoci.

COST	
Temporal: 6 mesos	**Econòmic:** Capex: 280k€ Opex: 50k€

Nom: "Creació Document de Seguretat"
Referència: INI/DOC - 002
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: Creació del document de seguretat de l'organització on s'indicarà expressament les mesures d'indole tècnica i organitzativa acord a la normativa de seguretat vigent que serà d'obligat compliment per el personal amb accés a les diferents classificacions de informació que trobarem dintre de la nostra organització. D'una banda, ens adequarem a la normativa vigent Espanyola en el tractament de les dades de caràcter personal, i a la resta de informació on no trobem legislació, s'indicarà expressament el tractament que podem realitzar els usuaris en funció del nivell descrit per cada informació.
També s'aprofitarà aquest document per conscienciar als usuaris de la importància de la seguretat de la informació i donar pautes i guies de com treballar de forma segura amb els diferents sistemes. A la seva vegada s'implementarà un calendari de revisió a mantenir durant la vigència d'aquest document per tal de mantenir la seva continua evolució i adequació als canvis en l'organització.
Descripció: De cara a poder gestionar i formar tot el personal del tipus de tractament que pot realitzar amb la informació de l'organització i dels diferents sistemes, es crearà un document que agruparà la normativa vigent de l'organització i es realitzaran formacions sobre el personal per tal de garantir un correcte tractament de la informació i reduir el riscos provinents d'un tractament incorrecte. A la seva vegada ens adequarem a la legislació vigent del país.
Dintre d'aquest document, s'aprofitarà per delimitar i aclarir les obligacions i responsabilitats de tot el personal intern de l'organització, com la relació contractual amb les autoritats o els tercers que treballin amb l'organització directament.

BENEFICIS

Pel departament S.I.:

- Creació política de seguretat sobre la informació i els sistemes.
- Creació dels diferents procediments de gestió sobre els usuaris, gestió d'accessos, tractaments autoritzats, etc.
- Anàlisi detallat dels procediments autoritzats a realitzar sobre les diferents informacions i responsables assignats sobre cada unitat de informació.
- Adequació a la legislació vigent.

Per l'organització:

- Conscienciació del usuaris sobre la seguretat de la informació.
- Guia de tractament i bones pràctiques.
- Minimització dels riscos per tractaments incorrectes.
- Tractament adequat i gestionat en funció del tipus de informació.
- Suport des de la direcció a la seguretat de la informació.
- Declaració de les obligacions i responsabilitats del personal intern.
- Declaració de les obligacions i responsabilitats del personal extern (clients o col·laboradors externs).
- Assignació clara de les responsabilitats relatives a la seguretat de la informació com la pròpia coordinació d'aquesta.

COST	
Temporal: 30 dies	**Econòmic:** 4,4k€

Nom: "Sistema de monitorització de Xarxa"
Referència: PRO/TEC - 004
Requeriments / Predecessors:

- PRO/TEC – 001
- PRO/TEC – 003

Objectiu: Gestió total del tràfic intern de la xarxa de l'organització i la connexió amb l'exterior o els diferents CPD's de l'organització a nivell internacional. Detecció activitats de processament de la informació no autoritzades.

Descripció: De cara a poder gestionar, monitoritzar i traçar tot el tràfic generat a la nostra organització, de cara a realitzar un control exhaustiu i a la seva vegada poder organitzar les mesures de seguretat corresponents per garantir la qualitat del servei a tots els usuaris, com l'anticipació dels problemes diversos sobre els sistemes o la infraestructura, cal implementar un únic sistema de monitorització que ens permeti realitzar totes aquestes tasques i establir les corresponents restriccions necessàries per poder garantir tant la qualitat com la seguretat de la informació.

Els sistemes han de ser monitoritzats i els successos de la seguretat de la informació enregistrats. El registre dels operadors i el registre de les fallades hauria de ser utilitzat per garantir la identificació dels problemes dels sistemes de informació. A la seva vegada, l'organització hauria de complir amb tots els requeriments legals aplicables per la monitorització i el registre d'activitats.

S'han d'implantar processos de supervisió de cara a mesurar l'eficiència dels controls establerts com l'ús que s'està realitzant tant de la xarxa com dels sistemes.

BENEFICIS

Pel departament S.I.:

- Monitorització complerta tant de la xarxa com de tota la infraestructura present a l'organització involucrada en el funcionament correcte dels diferents sistemes.
- Anticipació davant dels problemes e informació adient per tractar-los.
- Gestió optimitzada dels recursos.
- Anàlisi complert de rendiment i verificació de funcionament.
- Control total del tràfic intern i extern de la nostra xarxa.

Per l'organització:

- Major productivitat dels empleats donat la possibilitat de controlar els sistemes accessibles pel usuaris.
- Optimització del recursos.
- Reducció costos donat a la major optimització.

COST	
Temporal:	**Econòmic:**
2 mesos	5k€

Nom: "Classificació de la informació"
Referència: INI/DOC – 003
Requeriments / Predecessors:

- INI/DOC - 002

Objectiu: Classificar totes les fons de informació presents dintre dels sistemes actual de gestió de la informació utilitzats a l'organització de cara a mantenir clarament aquesta classificació i poder establir, organitzar i mantenir les diferents mesures de control i seguretat en funció d'aquesta classificació.
Descripció: De cara a poder realitzar la classificació, primer de tot es realitzarà un inventari de totes les fonts de informació present dintre de l'organització, de cara a realitzar posteriorment una classificació a partir d'unes directrius clares de classificació validades pel comitè de seguretat de l'empresa i la pròpia direcció que ens permeti agrupar i manipular aquest diferents tipus de agrupacions en funció del seu valor per l'organització.

BENEFICIS

Pel departament S.I.:

- Grups marcats pels diferents tipus de informació amb els seus controls i requeriments estipulats per cadascun d'ells.
- Classificació complerta de totes les possibilitats.
- Procediments d'actuació definits per cada cas.

Per l'organització:

- Foto clara dels tipus de informació manejats per tota l'organització.
- Major sensibilització del personal en funció de la classificació.
- Agilitat a l'hora de establir mesures de protecció segons tipus de informació.
- Coneixement detallat de tota la informació emmagatzemada a l'organització i control total sobre els seus tractaments.
- Coneixement dels riscos aportats per una "mala manipulació" d'aquesta informació.

COST	
Temporal:	**Econòmic:**
2 mesos	3k€

Nom: **"Depuració del inventari d'actiu"**
Referència: **INI/PROC - 001**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: De cara a optimitzar les futures inversions d'actius, cal realitzar una darrera passada sobre l'inventari actual de l'organització, de cara a controlar el 15% d'actius que no es troba correctament identificat o amb errades de classificació. En cas de detectar qualsevol ús inadequat d'aquest actius, ràpidament s'informarà al responsable corresponent de cara a solucionar la situació.
Descripció: Realització de la darrera volta de cicle sobre l'inventari d'actius de cara a controlar el 100% dels actius de l'organització.

BENEFICIS

Pel departament S.I.:
- Control del 15% actual "fora de norma".

Per l'organització:
- Optimització futures compres.
- Garantia d'ús correcte dels actius.

COST	
Temporal: 14 dies	**Econòmic:** 0,5K€

Nom: **"Tractament de la informació des de RRHH"**
Referència: **INI/PROC - 002**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: Confeccionar i mantenir vigents tots els procediments d'actuació relatiu al tractament de la informació en el departament de RRHH de l'organització de cara a donar cobertura a les diferents etapes de vida de la informació (abans, durant, canvi de posició o finalització) referent al personal de l'organització.
Descripció: Es definirà clarament els procediments d'actuació a implementar pel personal de RRHH amb la corresponent validació de la direcció pròpia de RRHH i la direcció general de l'organització dels diferents procediments que cal seguir per tractar la informació "sensible" que es pot tractar des de departament de RRHH. Dintre d'aquest procediments trobarem per exemple els procediments de tractament de la informació de caràcter personal, les condicions contractuals, o la pròpia formació del personal. A la seva vegada es revisaran tots els procediments d'actuació i relació del personal en funció de la seva relació amb l'organització.

BENEFICIS

Pel departament S.I.:
- Cap benefici apreciable directament.

Per l'organització:
- Definició clara dels procediments d'actuació del departament de RRHH.
- Compromís del propi departament per garantir la seguretat en les seves actuacions.
- Formació, conscienciació i capacitació continuada del personal

COST	
Temporal: 1 mes	**Econòmic:** 2 k€

Nom: **"Consolidació d'un comitè de Seguretat/Salut"**
Referència: **INI/ORG - 001**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: De cara a poder gestionar i organitzar la seguretat física i del entorn, en coordinació amb la seguretat de la informació, cal detectar les taques que cal mantenir constantment en relació a la seguretat/salut de l'entorn, realitzar la corresponent assignació de recursos per tal de realitzar aquestes tasques i establir els criteris d'actuació a nivell de seguretat en les àrees de treball. Aquest comitè haurà de presentar en cas necessaris els sub projectes a implementar anualment de cara a garantir la seguretat en tot moment. Inicialment es concentraran en optimitzar el control físic de les àrees de treball donat que s'ha detectat un nivell baix de control en aquest punt.
Descripció: Definició clara de la necessitat de realitzar tasques englobades dintre del perímetre de seguretat física i del entorn dintre de la nostra organització de cara a obtenir el recursos necessari per poder implementar-los i mantenir-los en el temps els diferents control o seguiment de les diferents tasques identificades.
Com podem veure clarament es tracta d'una iniciativa clara que modificarà l'organització i les tasques a portar a terme pel personal de l'organització amb l'objectiu de donar major cobertura al domini de la seguretat física i del entorn dintre de l'organització.

BENEFICIS

Pel departament S.I.:

- Cap benefici apreciable directament.

Per l'organització:

- Control i gestió de la seguretat física i del entorn de l'organització.
- Major organització a nivell de seguretat física.
- Delimitació clara de les diferents àrees i declaració dels criteris necessari d'accés a les mateixes.

COST	
Temporal: 1 mes	**Econòmic:** 3k€

Nom: **"Coordinació en la gestió de canvis"**
Referència: **INI/PROC - 003**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: De cara a poder assignar las responsabilitats i procediments interns i externs a nivell de comunicacions i gestió dels canvis dintre de l'organització, cal introduir la filosofia de tractament dels canvis de cara a optimitzar la coordinació entre els diferents departaments de l'organització o els serveis externalitzats fora de l'organització.
Descripció: De cara a donar un millor servei en la gestió de canvis, o la pròpia gestió de projectes dintre de l'organització, es realitzaran les corresponents formacions sobre el personal corresponent de l'organització de cara a la cerca d'una major transversalitat entre el diferents departaments de l'organització i fins i tot amb la gestió del recursos externs. Evidentment aquesta filosofia es mantindrà en la gestió diària de manteniment dels sistemes de la informació com en el manteniment de les pròpies comunicacions i es definiran rols específics dintre de tots els projectes nous que es comencin en l'organització, de cara a obtenir una màxima eficiència en el nivell de servei com a nivell de productivitat operacional.

BENEFICIS

Pel departament S.I.:

- Delimitació clara del rol de coordinació dels diferents recursos.
- Optimització dels recursos i procediments d'actuació.
- Supervisió i revisió del servei ofert.
- Documentació dels procediments d'operació.
- Gestió dels canvis als sistemes de la informació.

Per l'organització:

- Assignació clara de responsabilitats en les diferents tasques.
- Documentació dels procediments d'operació.
- Coordinació/optimització dels recursos
- Gestió complerta de tots el canvis.

COST	
Temporal: 2,5 mesos	**Econòmic:** 5k€

Nom: **"Definició requeriments Sistemes"**
Referència: **INI/DOC - 004**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: Establir uns criteris d'acceptació per nous sistemes de informació, actualitzacions i versions noves. Desenvolupar proves adequades dels sistemes durant les fases de desenvolupament o abans de la seva acceptació. A la seva vegada, cal monitoritzar l'ús de recursos, com la projecció de requisits i capacitats per garantir el futur del sistema durant la seva vida de servei.

Descripció: Es tracta d'una definició clara de la documentació clara a mantenir actualitzada en el moment de realitzar l'avaluació de nous sistemes de informació com la definició del manteniment i previsió de recursos per tota la vida estimada d'ús del sistema. Es definirà una fitxa clara amb tots aquest requeriments definits de cara a tenir-los definits durant tota la vida del sistema.

BENEFICIS

Pel departament S.I.:

- Garantir les necessitats dels diferents sistemes durant la seva vida útil.
- Definir uns criteris d'avaluació i adequació per noves necessitats.
- Gestionar l'evolució dels sistemes amb previsió.

Per l'organització:

- Millor control pressupostari de la vida d'un sistema i les seves necessitats futures.
- Criteris clars de selecció en funció de la línia definida per l'organització.
- Definició clara de les necessitats per part del negoci.
- Coneixement de les limitacions dels sistemes.
- Coneixement clar de les funcionalitats dels sistemes.

COST	
Temporal: 2 setmanes	**Econòmic:** 1,5k€

Nom: **"Gestió Backup de la informació"**
Referència: **INI/PROC - 004**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: Definir clarament les necessitats de salvaguarda de la informació dintre de l'organització confeccionant els diferents procediments d'actuació per tots els sistemes.
Descripció: De cara a establir aquest procediments d'actuació, es definiran els procediments corresponents i necessitats de salvaguarda de la informació com la correcta gestió de suports, per tal de gestionar completament la manipulació de la informació en tots els àmbits de l'organització. Caldrà revisar tots els sistemes actuals com les diferents fonts de informació e implementar uns documents específics per les necessitats futures.

BENEFICIS

Pel departament S.I.:

- Definició clara de les necessitats de salvaguarda.
- Definició dels procediments de manipulació relacionats de la informació.
- Control/Seguiment sobre les tasques de salvaguarda.
- Previsió de necessitat de recursos per salvaguarda.
- Reducció pèrdues informació per mala manipulació.

Per l'organització:

- Major garantia d'èxit en les tasques de salvaguarda de la informació.
- Reducció de les pèrdues de informació.

COST	
Temporal: 1 mes	**Econòmic:** 3k€

Nom: **"Revisió Política control d'accessos"**
Referència: **INI/DOC - 005**
Requeriments / Predecessors:

- **INI/DOC - 002**

Objectiu:

- Controlar els accessos a la informació.
- Garantir els accessos als usuaris autoritzats e impedir els accessos no autoritzats als sistemes de la informació, sistemes operatius, aplicacions o serveis de xarxa.
- Impedir els accessos d'usuaris no autoritzats i el compromís o robatori de informació i recursos per el tractament de la informació. Definició clara de les responsabilitats de l'usuari.
- Garantir la seguretat de la informació en l'ús de recursos de informàtica mòbil i teletreball.

Descripció: De cara a perfeccionar aquest apartat que trobarem sobre el propi document de seguretat, realitzarem una revisió i una sèrie de formacions focalitzades en aquest punt de cara a obtenir l'excel·lència en la gestió d'aquest apartat considerat com crític en el mon de la seguretat de la informació.

BENEFICIS

Pel departament S.I.:

- Revisió complerta dels accessos atorgats.
- Procediment clar pel tractament a implementar en relació als accessos en totes les seves variants.
- Registres organitzats de cara a una possible auditoria.

Per l'organització:

- Formació i conscienciació dels usuaris respecte a la política d'accés a la informació de l'organització.
- Revisió complerta de la situació actual.
- Coneixement clar de la filosofia d'autoritzacions a rebre de cara a sol·licitar accessos a la informació o els diferents serveis.

COST	
Temporal:	**Econòmic:**
20 dies	2,5k€

Nom: "Política de manteniment dels S.I."
Referència: INI/DOC - 006
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: De cara a garantir tota la vida útils dels sistemes de la informació des de la fase d'adquisició o desenvolupament i durant el seu manteniment, definirem una política clara a complimentar en el moment d'iniciar el projecte de implementació en el qual es definirà clarament:

- Els requisits de seguretat dels sistemes de informació.
- El tractament correcte de les aplicacions.
- Els controls criptogràfics (en cas necessari)
- La seguretat dels arxius de sistema.
- La seguretat en els processos de desenvolupament i suport.
- Com gestionar les possibles vulnerabilitats tècniques.

Descripció: De cara actualitzar la situació actual, aquesta iniciativa estarà dividida en dues fases, una primera en la qual es definirà clarament la política de l'empresa respecte els punts anteriorment comentats, i on es prepararan tots els documents necessaris a omplir i emmagatzemar durant la vida dels sistemes, i una segona fase a completar tota aquesta informació dels sistemes actuals de cara a arribar a una situació controlada dels sistemes de la informació que actualment es troben en funcionament o desenvolupament.

BENEFICIS

Pel departament S.I.:

- Definició clara dels criteris comuns de selecció de S.I.
- Fitxes complertes per gestionar la vida útil dels sistemes.
- Definició clara de les salvaguardes necessàries per cada sistema.
- Documentació estàndard e independent de l'equip de treball que va realitzar la implantació.

Per l'organització:

- Millor gestió Pro-activa del manteniment dels S.I. que es reflecteix directament en una reducció dels temps de parada del S.I.

COST	
Temporal:	**Econòmic:**
2 Mesos	6k€

Nom: **"Tractament de la gestió d'incidents en al seguretat de la informació"**
Referència: **INI/PROC - 005**
Requeriments / Predecessors: No presenta cap requeriment previ ni cap iniciativa predecessora necessària per tal de ser implementada.

Objectiu: De cara a obtenir el màxim de informació relacionada amb la gestió de la seguretat de la informació de la organització i poder gestionar eficientment aquest incidents, establirem una sèrie de procediments a seguir i que seran revisats i gestionats pel propi comitè de seguretat de l'organització de cara a adquirir la informació referent als successos o punts febles detectats i procedir a la gestió i millores de la seguretat de la informació.
Descripció: Es definiran els procediments d'actuació referents a la gestió d'incidents de seguretat de la informació i es formarà als equips de "helpdesk" de l'organització de cara a donar un correcte servei, evolucionant amb l'aprenentatge dels incidents passats, la recol·lecció d'evidències per possibles incidents futurs o la pròpia notificació dels successos o la documentació dels punts febles detectats. Amb aquests procediments d'actuació s'incorporaran els formularis (o aplicació) necessaris per poder realitzar aquestes tasques.

BENEFICIS

Pel departament S.I.:

- Definició complerta de la gestió de seguretat de la informació.
- Tractament des successos de seguretat.
- Aprenentatge dels incidents de S.I.
- Recopilació d'evidències.

Per l'organització:

- Millora substancial en el tractament dels incidents de seguretat de la informació.
- Major nivell de seguretat global.

COST	
Temporal:	**Econòmic:**
2 mesos	8K€

Nom: **"Control de compliment dels procediments/normes i requisits legals"**
Referència: **INI/AUDIT - 001**
Requeriments / Predecessors: **INI/DOC – 002**

Objectiu: Garantir el correcte compliment dintre de l'organització dels requisits legals deduïts de l'aplicació de la legislació aplicable com pla pròpia prevenció de l'ús inadequat de recursos de tractament de la informació en aquest àmbit, fins la garantia de compliment i la comprovació d'aquest, del correcte seguiment del estipulat en tots els procediments/Normes/Documents interns i amb aplicació directe sobre els sistemes de la informació i els propis empleats de l'organització.
Descripció: Es realitzaran revisions regulars de seguretat dels sistemes de la informació segons les polítiques de seguretat definides i s'auditaran aquest S.I. per garantir el compliment dels estàndards adequats de implantació de la seguretat com els controls per garantir el correcte seguiment dels diferents procediments/normes establerts.

BENEFICIS

Pel departament S.I.:

- Major seguiment de les tasques implementades.
- Preparació per possibles auditories oficials.

Per l'organització:

- Garantia de compliment dels procediments establerts.
- Detecció prèvia a les auditories oficials de possibles problemes.
- Aplicació del model de millora continua a la seguretat de S.I.

COST	**Temporal:**	**Econòmic:**
	1 mes	4k€

5.2.- Tractament Global Iniciatives

Realitzarem el tractament global de totes les iniciatives tant temporal com econòmicament per tal de poder conèixer ràpidament aquestes dues dimensions tan important per totes les organitzacions com són el temps i el cost econòmic de cara a la seva inclusió dintre principalment de la gestió del departament de S.I. de l'organització.

5.2.1- Planificació temporal integrada en el Pla Director

En aquest apartat tractarem el conjunt de projectes enumerats a l'apartat anterior de forma global per la nostra organització i com quedem enquadrades en els diferents anys d'actuació del mateix. D'aquesta forma podem observar ràpidament com quedaria la planificació dels pròxims 4 anys:

Any 2013:

- PRO/TEC – 001
- PRO/TEC – 002
- PRO/TEC – 003
- PRO/TEC – 004
- INI/PROC - 003

Any 2014:

- INI/DOC – 001
- INI/DOC – 002
- INI/DOC – 003
- INI/DOC – 004
- INI/PROC - 005

Any 2015:

- INI/PROC – 001
- INI/PROC – 002
- INI/ORG – 001
- INI/PROC – 004
- INI/DOC – 005
- INI/DOC – 006
- INI/AUDIT - 001

L'**any 2016**; estarà fitxat com un període d'absorció de possibles retards dels projectes e iniciatives anteriorment plantejats, i a la seva vegada es realitzarà l'auditoria complerta de la implantació de tots els projectes indicats en aquest PDS, de cara a garantir, que a la finalització del PDS (durant l'any 2016) tot els objectius establerts han estat satisfets.

	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				

Com podem observar clarament, aquesta planificació esta orientada principalment a implementar inicialment els projectes que aporten millores tecnològiques sobre l'organització i redueixen el risc detectat actualment; a continuació s'arranca una fase de creació de normes i procediments a posar en marxa dintre de l'organització (amb la implementació sobre els sistemes vigents en aquell moment) i per últim una fase d'adaptació a la norma ISO 27002 per acaba de garantir els objectius marcats per la direcció de l'organització a la finalització del període de vigència d'aquest PDS.

5.2.2.- Planificació econòmica de les iniciatives del Pla Director

En aquest punt veurem la planificació total de la implementació del conjunt de projectes com el seu cost econòmic global de cara a la realització dels diferents pressupostos de l'organització. D'aquesta forma tindrem clares les partides necessàries a implementar pel Budget de cada any, i el cos final estimat per la implementació de tots els projectes presentats en aquest PDS:

Any 2013: **226k€**
Any 2014: **296k€**
Any 2015: **19k€ (+ 50k€ opex)**
Any 2016: **4k€ (+ 50k€ opex)**

Cost total implementació projectes PDS: 545k€ (+ 50k€ opex per any)

Com podem observar clarament en l'organització i planificació dels projectes, el cost econòmic fonamental recau sobre els dos primer anys d'implementació principalment perquè s'han d'implementar els projectes tècnics necessaris per reduir els riscos detectats mitjançant l'anàlisi de riscos realitzat i la preparació del BCP (Business Continuity Plan) que l'organització vol implementar el mes aviat possible de cara a poder obtenir els beneficis de seguretat que incorpora. Evidentment la resta de projectes, estan enfocats a millorar la qualitat dels controls dels diferents dominis establerts per l'ISO a la qual es vol arribar en una situació de sol·licitud en la finalització d'aquest PDS.

5.3.- Anàlisi d'impacte dels projectes sobre la seguretat

De cara a poder comprendre de forma molt ràpida com afecta la implementació d'aquest projectes sobre les diferents dimensions analitzades sobre l'anàlisi de riscos, com l'impacte sobre els dominis i objectius de control aportats per la ISO/IEC 27002:2005; prepararem una taula resum dels projectes indicant els beneficis aportats per cada un d'ells:

- **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
- **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
- **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

5.3.1.- Evolució Risc / Impacte Potencial

A raó principalment de l'aplicació dels projectes tècnics que es portaran a terme durant el primer any d'aquest PDS més la creació del document de seguretat de l'organització i el Business Continuity Plan per la nostra organització (sense oblidar iniciatives puntuals que fan millorar alguns valors de las dimensions de seguretat com podria ser la gestió del backup, la revisió de la política d'accessos entre d'altres); aconseguirem reduir els valors **del Impacte Potencial** sobre la nostra organització, i per tant observarem un reducció sobre el risc al qual estem exposats.

Per tal d'obtenir aquest resultats, hem tornat a realitzar tots els càlculs de l'anàlisi de riscos però aplicant els beneficis que incorporem cadascun dels projectes plantejats sobre les 5

dimensions de seguretat analitzades, ja que gracies als projectes aconseguim reduir en alguns casos la freqüència d'ocurrència però majoritàriament observem reduccions sobre l'impacte causat en cas de materialització.

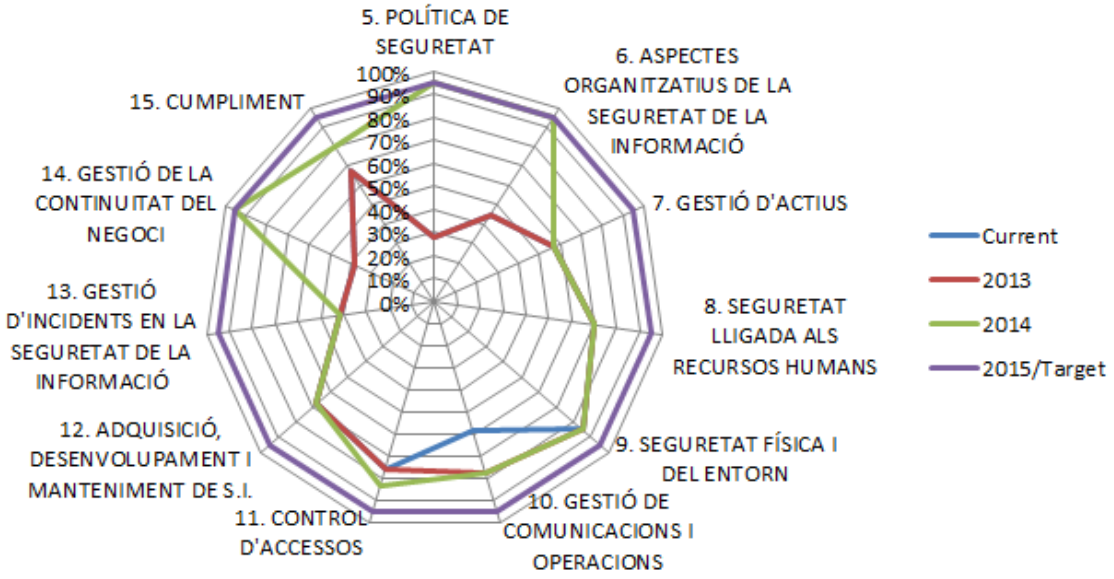
De cara a mostrar aquest resultats; utilitzarem el mateix quadre que van utilitzar en l'apartat de l'anàlisi de riscos d'aquest document per mostrar l'impacte potencial i a continuació indicarem com queden aquest valors un cop aplicats els diferents projectes indicats per aquest PDS i que fan reduir alguns dels valors observats a l'impacte potencial:

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

Com podem observar gracies als projectes tècnics implementats i a les iniciatives especifiques anteriorment comentades; podem observar que les dimensions de "Confidencialitat" i "Disponibilitat" presenten la major reducció sobre els seus valors de impacte potencial; com la dimensió de "Integritat" que es veu reforçada per varies iniciatives especifiques com som la gestió de salvaguardes i la definició de requeriments. A nivell de "Autenticitat" i "No-Repudi" veiem que els valors també milloren però es menor mesura respecte les altres dimensions donat l'indole dels diferents projectes aportats per aquest PDS.

5.3.2.- Evolució Nivell Compliment ISO

A raó de la planificació marcada pels diferents projectes definits en aquest PDS, i donada la implicació sobre cada domini ISO de cadascun dels projectes; podem observar la següent evolució del nivell de compliment dels controls ISO:



5.4.- Canvis Organitzatius presentats al PDS

Dintre de les iniciatives/projectes plantejats per aquest PDS, veiem clarament una iniciativa (INI/ORG – 001) que implica certs canvis a implementar dintre de l'organització de cara a la realització de la gestió complerta i tractament de la seguretat en la nostra organització.

Com ja hem pogut observar a llarg de tot el document, la nostra organització ha començat un procés d'evolució a nivell de seguretat de la informació, donant la importància i el suport des de la direcció que requereix per la seva implementació, i per tant caldrà consolidar aquesta àrea d'actuació i servei a nivell de l'organització mitjançant la consolidació d'un comitè de seguretat (que englobaria tant les àrees de seguretat de la informació, com la seguretat física i salut que ja existeixen dintre de l'organització) per tal de establir les corresponents tasques, obligacions i serveis a realitzar e implementar per poder garantir plenament el desenvolupament correcte de la seva missió fonamental com serà la gestió de la seguretat. En aquest procés de consolidació, es definiran tasques concretes que requeriran recursos per tal de poder mantenir i evolucionar aquesta gestió de la seguretat, per tant veiem clarament que el suport de la direcció resultarà clau per la seva correcta implementació com l'aportació dels recursos necessaris (personals com econòmics) per poder garantir la implementació i el manteniment dels procés de evolució a nivell de seguretat que estem plantejant dintre de la nostra organització.

Com ja hem enumerat en repetides ocasions, els beneficis d'utilitzar aquesta estructura organitzativa a nivell de seguretat dintre de l'organització ens reportarà tots els beneficis

comentats al llarg d'aquest document però requereix els corresponents recursos per tal de poder implementar-los i mantenir-los en tot moment. Per tant resulta vital per la consecució d'aquest objectius, el compromís de la direcció per estudiar la necessitat dels recursos requerits com la seva aprovació i disposició un cop estiguin validats.

El procediment de comunicació amb la direcció per la sol·licitud d'aquest recursos, serà la presentació d'un document confeccionat pel responsable operatiu d'aquest PDS de les necessitats pertinents un cop estigui consolidat el comitè de seguretat i definides totes les tasques a implementar, aportant les necessitats exactes a nivell organitzatiu com la justificació d'aquestes necessitat en temps (ja sigui per la implementació o per tota la vida de l'estructura de seguretat) i aquesta serà avaluada i contestada pel comitè de direcció en un terme de 15 dies hàbils. Com veiem aquest plantejament va enfocat principalment a la sol·licitud de recursos "humans" ja que tota la resta de recursos necessaris per la implementació de les iniciatives amb estat contemplats dintre de la valoració dels diferents projectes.

Aquest mètode de tractament de les futures necessitats ha estat validat i aprovat expressament amb el comitè de direcció de s'ha compromès a realitzar des del departament de RRHH la definició dels nous post de treball o l'assignació de les noves tasques que aquest nou comitè de seguretat dictamini com necessàries.

5.5.- Conclusions

Com hem pogut observar en aquest apartat, s'ha preparat una proposta complerta dels diferents projectes que considerem resulten interessants implementar sobre la nostra organització de cara a anar alineats amb els resultats observats en l'anàlisi de riscos i l'anàlisi de compliment dels controls ISO/IEC 27002:2005 que hem realitzat en els apartats anteriors d'aquest document; per tal de millorar la situació actual de l'organització; reduint el risc i l'impacte al qual l'organització es troba exposat i millorant el nivell de compliment fins arribar als objectius marcats des de la direcció de l'organització per els pròxims 4 anys (vigència d'aquest PDS).

Com podem observar, hem pogut veure que la execució dels diferents projectes plantejats ens mostrarà com evoluciona el risc i el impacte de materialització, així com el nivell de compliment dels diferents dominis de la norma ISO 27002. Com podem veure clarament, l'objectiu final, després dels 4 anys de procés d'implementació de les diferents iniciatives i projectes; es anar evolucionant cap a un nivell de maduresa optimitzat.

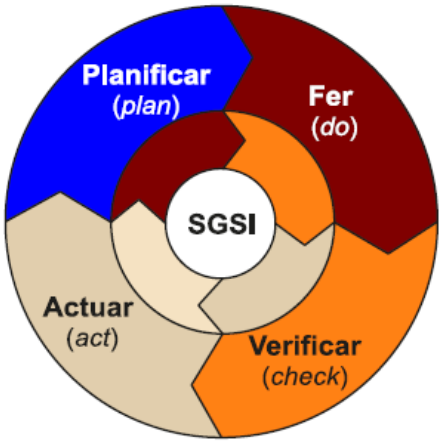
Aquesta implicació dels diferents projectes queda plasmada sobre els àmbits als quals aportat benefici cadascun dels projectes i de forma gràfica podem observar l'evolució anual que l'organització realitzarà a nivell dels compliment dels diferents dominis fins arribar als objectius marcats des de la direcció de l'organització.

Cal destacar, que el darrer any d'aquest PDS, presenta un període d'auditoria complerta per analitzar que s'ha implementat correctament totes les iniciatives i verificació de que hem arribat al nivell desitjat que d'una banda ens servirà per corroborar els nostres objectius inicials, i ens donarà un marge de temps per poder implementar modificacions o noves iniciatives en cas de detectar qualsevol deficiència abans d'arribar a la data límit en la qual l'objectiu de l'organització ha d'estar complert. Aquest objectiu, com ja s'ha comentat al llarg de tot el document, no es altre que garantir a la finalització d'aquest PDS, un nivell acceptable de risc e impacte sobre la nostra organització i un nivell de compliment de la norma ISO 27002 de "Gestionat i mesurable" (95% de compliment) de cara a estar en situació de sol·licitar la certificació en cas de que la direcció volgués en l'any 2017 obtenir-la, tal i com s'ha indicat expressament a l'inici d'aquest PDS.

6.- Glossari

Cicle de Deming: També conegut com a cicle PDCA (Plan Do Check Act), que és un procés iteratiu de qualitat en quatre fases:

- **Plan:** establir els objectius i processos necessaris per a aconseguir els resultats esperats.
- **Do:** implantar els processos nous.
- **Check:** mesurar els processos nous i comparar els resultats obtinguts amb els esperats.
- **Act:** analitzar les diferències entre els resultats obtinguts i els esperats per a saber-ne les causes i plantejar-hi millores.

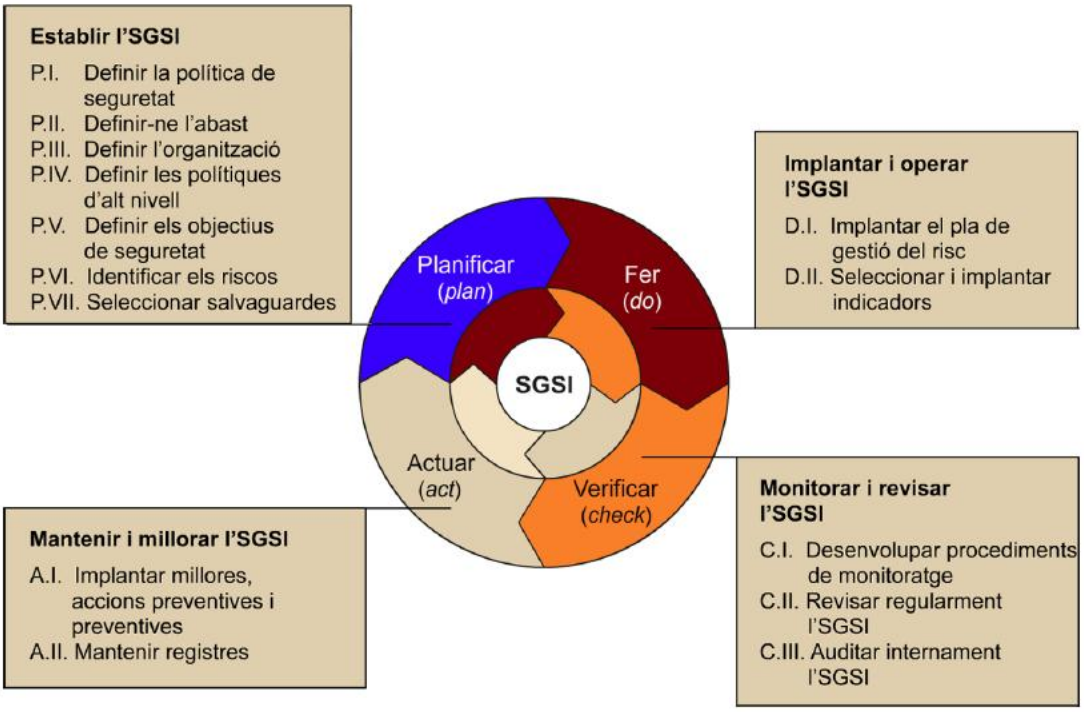


Cicle de Deming o cicle PDCA

Si apliquem aquest procés sobre la pròpia gestió de la seguretat de la informació ja sigui mitjançant la implantació d'un sistema gestor de la seguretat de la informació (SGSI) o la pròpia generació d'un pla director (PDS)com aquest que estem realitzant; que te com objectiu gestionar la seguretat de la informació (al igual que un sistema gestor con seria un SGSI) per tal de garantir i evolucionar la seguretat de la nostra organització.

Dintre d'aquesta filosofia de treball, podríem descriure una sèrie de fases o apartats en cada una de aquestes quatre fases principals que ens garantiran arribar al nostre objectiu final i garantir tot una sèrie de indicatius per poder mesurar en tot moment aquesta evolució. En concret aquestes fases pertanyen a la pròpia creació d'un SGSI de cara a una posterior certificació. Podrien dir que es tractaria d'un pas paral·lel al nostre PDS, molt comú en la part pública o proveïdors de serveis a tercers.

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



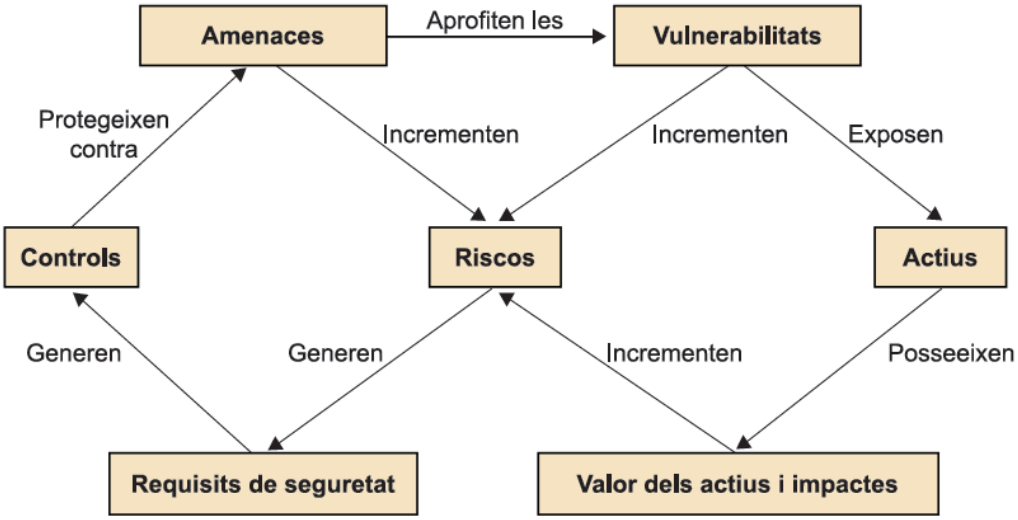
Actius: són tots els elements que té l'organització i que s'analitzen durant el procés de l'anàlisi de riscos. Cal destacar que per a actiu s'entén tot element que requereix l'organització per a fer les activitats de negoci que li són pròpies.

Amenaces: són les situacions que es poden arribar a donar en una organització i que desembocarien en un problema de seguretat.

Vulnerabilitat: són les diferents debilitats que presenten els actius identificats i que són aprofitats per les amenaces per a provocar un dany a nivell de seguretat.

Impacte: Al mon de la seguretat de la informació, es defineix com les conseqüències que provoca en l'organització el fe que una certa amenaça, aprofitant una determinada vulnerabilitat, afecti un actiu.

Risc: Dintre de les diferents definicions que podem observar per el terme "risc" dintre de la seguretat de la informació; podem dir que es tracta d'una combinació de les de les amenaces que aprofiten les vulnerabilitats existents generant un impacte contra els actius de l'organització. A continuació; podem observar un petit gràfic de com s'interrelacionen tots aquest conceptes.



El gràfic mostra les relacions que es creen quan es parla de seguretat de la informació i quan es pretén minimitzar els **riscos** a què està exposada una organització.

Una vegada es te clar tots aquest conceptes dintre d'una organització, podrem tenir clara quina es la situació, coneixent a quines amenaces podem ser sensibles en funció de les vulnerabilitats existents pels nostres sistemes o serveis de la informació i quin impacte o risc sofrir en cas de materialització de les mateixes. A la seva vegada es important tenir clar en tot moment aquest conceptes, per poder mitigar-los o afrontar-los y poder tornar ràpidament a una situació d'estabilitat.

Risc residual: A nivell de la seguretat de la informació, parlarem de risc residual com el risc resultant una vegada s'han aplicat mesures o controls per tal de reduir la vulnerabilitat o l'impacte que presenta un actiu abans d'aplicar les mesures. De cara a evitar un cost desmesurat en controls es sol aplicar aquest principi: