Màster Interuniversitari en Seguretat de les TIC (MISTIC)

Treball Final de Màster
Primavera 2012

Elaboració d'un Pla de Seguretat de la Informació

Guillem Gimeno Domenech

Consultor: Arsenio Tortajada Gallego

Barcelona, 11 de gener de 2013

Resum Executiu

Introducció

En l'actualitat, s'accepta que la informació és l'actiu més important que qualsevol organització té sota el seu control.

L'ISO 27001:2005 es la Norma Internacional de Informació sobre Gestió de la Seguretat(SGSI) i proporciona una referència definitiva per al desenvolupament d'una estratègia de seguretat de la informació. A més a més, una exitosa certificació d'aquesta norma es la confirmació de que el sistema empleat per la organització compleix amb els estàndards internacionals reconeguts.

Aquesta norma, serà gairebé una obligació per a qualsevol empresa que desitgi competir en el mercat, degut a que si es volen interrelacionar sistemes de clients, control de stock, facturació, comandes, productes, ... es deuen exigir uns nivells concrets i adequats de seguretat informàtica per evitar fuites de seguretat i possibles pèrdues econòmiques o de prestigi per a la organització.

El propòsit d'aquesta norma, no està orientada només a un desplegament tecnològic, sinó també a aspectes organitzatius. La Seguretat de la Informació es una qüestió de tota la organització i creua les fronteres departamentals, es tracta d'alguna cosa més que mantenir una petita quantitat d'informació en secret.

Motivació

La implantació d'un SGSI en les organitzacions genera múltiples beneficis, que es poden resumir en:

- Credibilitat: degut a la confiança dels clients en quant a la protecció de la seva informació
- Estalvi: degut a la reducció de costos derivats de possibles pèrdues ocasionades per incidents no controlats.
- Garantia: satisfacció de requisits davant entitats reguladores.
- Compromís: demostrat en tots els nivells de la organització.

Enfocament

En el present projecte es pretén donar una solució de seguretat adequada a l'empresa XXX S.L, prenent com a base els estàndards internacionals.

La primera fase del projecte, ens dona una visió general de la situació actual de l'empresa, a partir de la qual s'obtenen els coneixements necessaris per a triar un enfocament per a la seva realització. En la segona fase establim les bases per a realitzar aquest Sistema de Gestió de la Seguretat de la Informació, es marquen uns objectius, es busca el suport de la direcció i s'estructura la organització per tal de aconseguir aquests objectius.

En la tercera fase es realitza l'anàlisi de riscos, on s'identifiquen els actius essencials per a que la organització funcioni correctament, s'analitzen les vulnerabilitats i l'impacte de les possibles amenaces.

A la quarta fase s'avalua el nivell de compliment dels controls ISO 27002:2005, un estàndard que agrupa un total de 133 controls o salvaguardes sobre les bones pràctiques per a la Gestió de la Seguretat de la Informació. En la cinquena fase es presenten les propostes de millora i el seu cost de implementació envers aquest mateix estàndard.

Conclusions

El Sistema de Gestió de Seguretat de la Informació es defineix per a cada organització en base als riscos a la que està exposada i els aspectes intrínsecs del seu funcionament.

Per a l'establiment de la seguretat de la informació, es consideren tres pilars fonamentals; tecnologia, processos i les persones. Les empreses solen invertir grans sumes de diners en tecnologia i definició de processos, descuidant el personal que ho haurà de gestionar, raó per la qual es fonamental conscienciar i fomentar la cultura de la seguretat de la informació als treballadors.

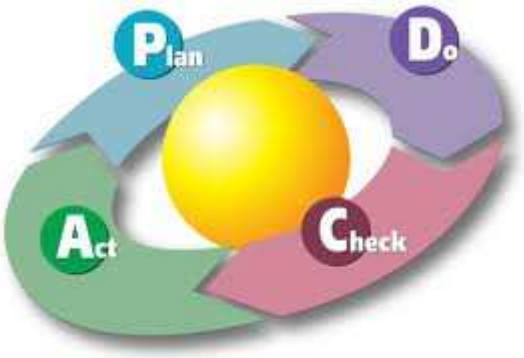
Tot plegat porta a la conclusió que la seguretat no és un producte, sinó que es tracta d'un procés, una activitat que ha de tenir continuïtat. En concret, es tracta del procés de mantenir l'organització en un entorn de risc gestionat, en el llindar de risc desitjat, mitjançant un seguiment continu i una inversió proporcional i justificada.

Índex

Fase 1: Contextualització i documentació.

1.1 Introducció.

El Pla Director de Seguretat és un dels elements clau amb què ha de treballar el Responsable de Seguretat d'una organització. Aquest pla constitueix el full de ruta que ha de seguir l'empresa per gestionar d'una forma adequada la seguretat, permetent no només conèixer l'estat de la mateixa, sinó en quines línies s'ha d'actuar per millorar-la. Estem parlant per tant d'un model PDCA (Plan-Do-Check-Act).



El marc legal ha reflectit la importància de la seguretat de la informació (a nivell de l'estat espanyol, lleis com la 11/2007 ho demostren). La seguretat no és per tant un aspecte opcional, sinó que ha de ser inherent a les activitats de la pròpia empresa, i constitueix un punt de partida ineludible per a tota organització en l'actualitat.

El plantejament del projecte serà per tant, establir les bases d'un Pla de Director de Seguretat per a l'empresa. Simplificant, i com anirem veient, el nostre procés serà el següent:

•Analitzar i detallar el nostre inventari d'actius.

•Estudiar les amenaces a què estan exposats.

•Estudiar el impacte potencial d'aquestes amenaces.

•Proposar un pla d'acció per lluitar contra aquestes amenaces.

•Avaluar el impacte residual un cop aplicat el pla d'acció.

Intencionadament, la llista anterior no contempla aspectes organitzatius, que tot i així, tocarem al llarg d'aquest projecte.

1.2 Presentació i descripció de l'empresa.

L'empresa XXXXXX es una organització exclusivament dedicada a la venta de productes tèxtils online.

Actualment distribueix els seus productes a tota la Península Ibérica a més de quatre països de la UE: França, Alemanya, Anglaterra i Itàlia.

L'empresa compta amb seu a diversos països. Una de les seus situada a Barcelona, que esdevindrà la base d'aquest treball.

Les seus no es no tenen una infraestructura per a comunicar-se entre si, ja que funcionen com organismes independents en el seu país, no obstant es realitzen reunions mensuals entre els directors de les seus per a debatre temes relacionats amb l'empresa.

L'abast d'aquest treball serà exclusivament per a la seu de Barcelona, incloent-hi tots els departaments que hi són presents a la mateixa.

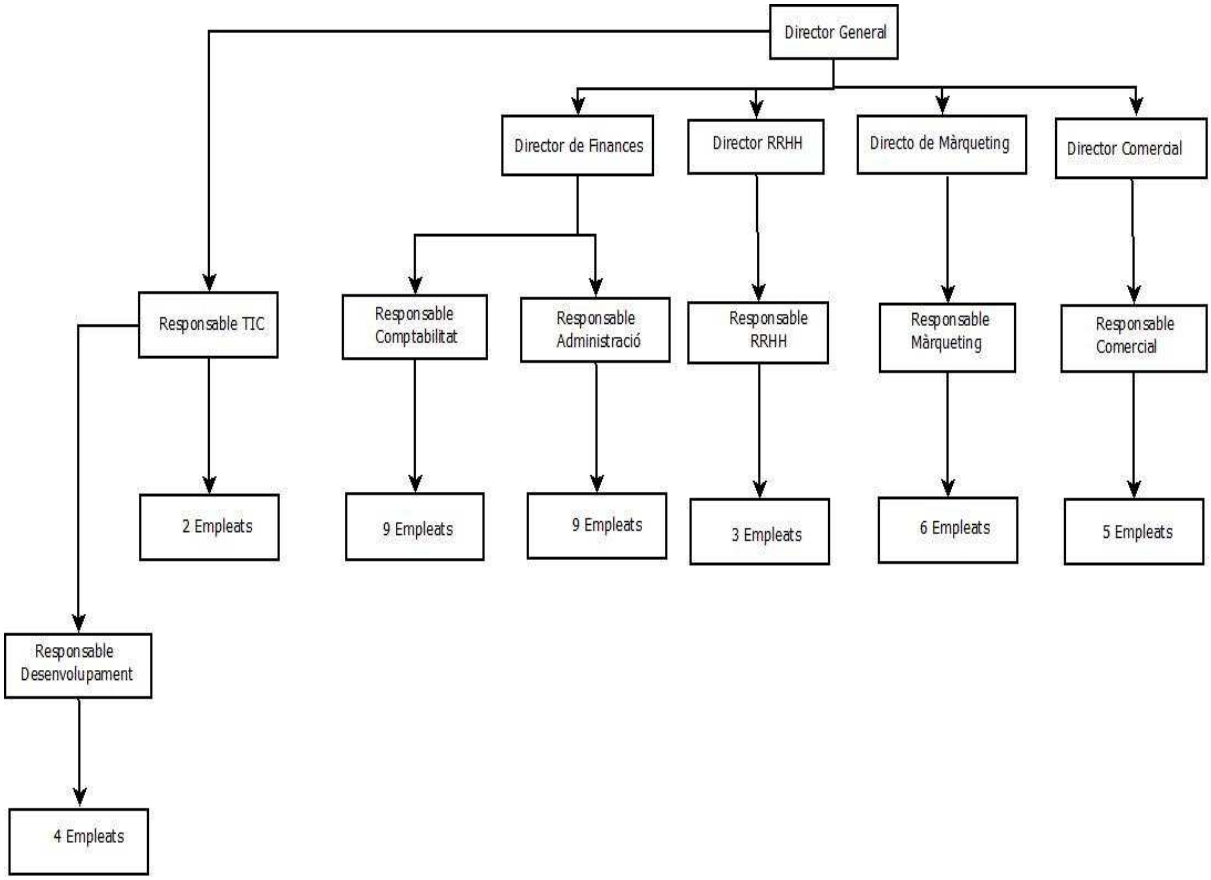
1.2.1 Organització del personal

En aquesta seu de Barcelona, hi treballen empleats de tots els departaments, ja que tot i ser una companyia global, cada seu funciona d'una manera independent a les demés.

L'empresa compta amb 50 empleats en aquesta seu a Barcelona, distribuïts en dues plantes(tercera i quarta planta) dins d'un mateix edifici, en el qual també s'allotgen dues empreses més. Les diferents plantes estan connectades mitjançant unes escales i dos ascensors.

Entre aquests 50 empleats, hi ha 3 informàtics al departament de xarxes i anàlisi de sistemes, 5 programadors, encarregat de resoldre incidències amb la web i la constant millora de la mateixa i més treballadors dels departaments de màrqueting, comercial, administració, recursos humans, comptabilitat i direcció.

Esquema de personal:



1.3. Estat Inicial de la seguretat

Actualment, l'empresa no compta amb un departament de seguretat específic, ni amb un SGSI certificat.

El director de seguretat de l'empresa, és a més, un dels tres informàtics que hi treballen. És l' encarregat de comprovar que es compleixin adequadament les necessitats de seguretat en les tasques que s'han de realitzar.

Organització de la seguretat de la informació

Com es comenta anteriorment, en aquesta empresa no trobem un SGSI prèviament implantat, no obstant, la responsabilitat recau com a cap de seguretat en un dels informàtics, però es troben polítiques i procediments de seguretat heretats d'altres seus de la companyia.

Tant en la tecnologia i comunicacions com en l'àmbit de recursos humans, es té sempre present la seguretat de la informació.

Gestió d'actius

L'empresa compta amb inventaris d'actius que s'actualitzen mensualment, detallant la seva funcionalitat i importància dins de la organització. No obstant, aquests actius no estan classificats com demanda la normativa ISO.

Els comercials i el personal de màrqueting disposen d'un portàtil cadascun a més del sobretaula de l'empresa per a fer desplaçaments .

Pel que fa al software, tots aquests ordinadors, disposen de programes amb llicencia de processament de textos, descompressió d'arxius i antivirus. El departament de màrqueting a més a més disposa d'ordinadors amb llicències de Photoshop.

Els departaments de comptabilitat i Administració i Recursos Humans utilitzen un software propi, adaptat per a gestionar els propis recursos.

La pàgina web de la companyia a Espanya està desenvolupada en llenguatge PHP i està allotjada a un domini .es

Seguretat lligada als recursos humans

Abans d'entrar a treballar, la persona que es vol contractar ha de signar una sèrie de polítiques de confidencialitat i no divulgació, per tal d'evitar la fuita d'informació de l'empresa.

El mateix procediment és aplicat a empreses externes que es subcontracten per a la realització de certs treballs puntuals.

Tant treballadors com terceres parts associades, són posats al dia de les possibles amenaces de seguretat mitjançant l'entrega de documents informatius relacionats.

D'altra banda, no es contempla una política definida i estructurada per a gestionar la baixa d'una persona o empresa. Simplement es comprova la revocació de permisos i la devolució d'actius un cop han abandonat l'empresa.

Seguretat Física i del entorn.

L' entrada a l'edifici es realitza mitjançant una targeta de referència magnètica amb el nom i cognom de la persona i el logotip de l'empresa. A més també es disposen de targetes per a convidats i

personal temporal on hi consta només el logotip. No obstant només està vigilada l'entrada a l'edifici, un cop a dins una persona amb acreditació d'una altra empresa, no ha de passar per cap control més.

La sala de servidors està tancada amb clau i només hi tenen accés els tres informàtics de l'empresa.

Aquesta sala es troba a la quarta planta, al final de la sala a mà esquerra, prenent com a referència la porta d'entrada.

Cal destacar la presència de tres aparells d'aire condicionat dins de la mateixa, que fan baixar la temperatura ambient per a un millor rendiment.

L'empresa disposa d'un sistema de SAIs, que permetrien als servidors seguir treballant durant un període de 3 hores.

Gestió de comunicacions i operacions

Els equips de l'empresa es divideixen en quatre nivells, entre els quals hi trobem un Firewall.

Xarxa externa: Accessible des de l'exterior, l'empresa compta amb un servidor amb un host IDS on s'allotja la pàgina web i la BBDD.

Xarxa interna: És una DMZ, on es troba un servidor DNS, un servidor de correu, un servidor proxy y un servidor web intern.

Red interna de serveis: Servidor de BBDD, servidor d'aplicacions, servidor de directori LDAP, servidor d'impressió.

Per últim ens trobem la xarxa d'usuaris. composta d'ordinadors de sobretaula i portàtils.

Control d'accés

Cada usuari de la companyia té assignat un usuari nominal de domini amb el que accedirà al seu ordinador.

Per accedir als recursos compartits de sistema, s'utilitza un altre usuari, donat d'alta a LDAP, el qual tindrà els permisos pertinents depenent de les funcionalitats i recursos que hagi de sol·licitar l'usuari.

La administració d'aquests usuaris pertany al departament d'informàtica(xarxes).

Les claus d'aquests usuaris consten d'un mínim d'onze caràcters, on s'han d'incloure números i lletres. Aquestes claus expiren cada trimestre i han de ser substituïdes per claus que no hagin estat utilitzades anteriorment.

Adquisició i manteniment de sistemes de la informació

Per evitar canvis en l'entorn de producció, els programadors disposen d'entorns virtualitzats per a la realització de proves. Aquests entorns els generen els informàtics responsables del departament de xarxes, assignant permisos als usuaris nominals dels programadors per a accedir-hi, evitant així l'accés no autoritzat al software que es desenvolupa en aquells moments.

D'altra banda, el software genèric als sistemes operatius es instal·lat pel departament de xarxes, evitant així que els usuaris instal·lin software que pugui perjudicar la seguretat i mantenint una unanimitat en el software.

Gestió d'incidents en la seguretat de la informació i Gestió de la continuïtat del negoci.

No existeixen plans específics documentats que detallin els procediments concrets per a la continuïtat del negoci. Els propis treballadors de l'empresa en cas de pèrdua d'informació tenen assolides les directrius a seguir per a aconseguir la continuïtat del negoci amb el menys impacte possible.

Compliment

Tots els usuaris que es donen d'alta a la web, queden registrats a la base de dades. Aquesta informació no és accessible al gruix dels treballadors, però si als informàtics, tant als programadors com als responsables de xarxes.

Fase 2: Objectius del Pla Director

2.1 Introducció

Ara que coneixem la metodologia pel que fa a implementar, mantenir i millorar la gestió de la seguretat en l'empresa, així com la guia per realitzar una anàlisi de riscos consistent, hem de reflexionar sobre què pretenem amb el Pla Director.

Encara que sembli un punt trivial, és un aspecte clau. El Pla Director no té interès per si mateix, sinó és dins d'un marc organitzatiu, on es valora la seva importància, i alhora l'organització posa els mitjans perquè els resultats que s'extreguin del Pla Director es puguin dur a terme.

2.2 Objectius del Pla Director.

L'organització fa saber que amb la implantació del Pla Director, es volen identificar les necessitats futures, per tal que la seguretat ajudi a aconseguir els objectius del negoci.

Es volen definir les estratègies i polítiques cooperatives TIC, donant especial importància a la seguretat de la Informació. Per a acabar definint un model integral de gestió de riscos basat en els estàndards ISO 27001 i 27002.

2.3 Suport per part de la organització.

Es fa saber a la organització, que el Pla de Seguretat comprendrà, no només mesures tècniques sinó també mesures polítiques i organitzatives dins de la companyia, per tal d'assolir els objectius corporatius de millora desitjats. Per assolir-se aquests objectius, caldrà primerament conscienciar tots els empleats de la organització, mitjançant la creació d'una Política de Seguretat.

Amb la finalitat d'elaborar una política de Seguretat adequada per a l'empresa, es deuran prendre responsabilitats des de la direcció.

La companyia haurà de saber que tots els Directors Generals, Gerents i titulars d'unitats de l'organització, seran responsables de la implementació de la Política de Seguretat de la Informació, així com el compliment de la mateixa per part del seu grup de treballadors.

Les màximes autoritats de l'empresa, hauran d'aprovar aquesta política i seran responsables de la autorització de modificacions.

Altrament, es crearà una estructura interna amb responsabilitat directa sobre la seguretat de la informació.

La direcció haurà d'aprovar l'estructura organitzativa i l'assignació de funcions. A més de donar suport per a dotar les persones amb responsabilitat en la matèria de l'autoritat i temps necessaris per a exercir les seves funcions dins de la companyia.

Es crearà un Comitè de Seguretat de la Informació, que serà l'encarregat d'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 i que supervisarà i aprovarà el desenvolupament del pla de continuïtat del negoci.

Aquest comitè contarà amb un Responsable de Seguretat de la Informació, juntament amb els responsables de les àrees de Màrqueting, Administració, Comercial, Recursos Humans, Comptabilitat i Tecnologies i Comunicacions.

Estructura organitzativa exposada:

<table>
<tr><td colspan="4">Comitè de direcció (Nivell estratègic)

- Visió estratègica
- Gestió de recursos</td></tr>
<tr><td colspan="4">Comitè de Seguretat de la Informació(Nivell Tàctic)

- Lideratge
- Gestió de Riscos
- Comunicació</td></tr>
<tr><td colspan="4">Responsable de Seguretat de la Informació (Nivell tàctic i operatiu)

- Coordinació
- Control i report</td></tr>
<tr><td>Responsable RRHH</td><td>Responsable Comercials</td><td>Responsable Màrqueting</td><td rowspan="2">(Nivell Operatiu)</td></tr>
<tr><td>Responsable Administratius</td><td>Responsable Comptabilitat</td><td>Responsable TIC</td></tr>
</table>

En aquest esquema es pot observar com aquest pla director implicarà tota la companyia.

Per la seva part, el Comitè Director, estarà format per el director de la oficina i els quatre subdirectors de la mateixa. Aquests s'encarregaran de fer de la seguretat de la informació un punt de la seva agenda.

Seran els encarregats de determinar el llindar de risc acceptable en matèria de seguretat.

Les decisions preses pel comitè de Direcció en matèria de Seguretat de la Informació, seran recollides en acta.

El Comitè de Seguretat de la Informació, serà l'encarregat d'assignar rols i funcions en matèria de seguretat. Aquest comitè estarà format permanentment per els responsables dels diferents departaments de l'empresa: Recursos Humans, Administració, Comercial, Comptabilitat, Màrqueting i el Responsable de les TIC, un total de 6 persones. No obstant, puntualment s'hi podrien afegir el responsable de Seguretat Física i de Manteniment(neteja, avaries, ...), que actualment són personal extern a l'empresa, però podria ser requerida la seva presència per a temes puntuals.

Inicialment, aquest comitè es reunirà sovint (cada dues setmanes aproximadament). Un cop superades les primeres fases, es podrà celebrar una reunió cada dos o tres mesos.

Per la seva banda, el responsable del Comitè de Seguretat de la Informació, serà el responsable de les TIC, que fins ara havia estat la única persona implicada en aquest àmbit.

Fase 3: Estat del Risc: Identificació i valoració dels Actius i Amenaces

3.1 Introducció.

Els actius son el elements que es deuen protegir envers riscos i amenaces per a assegurar un correcte funcionament del negoci.

La primera etapa cap a la consecució del Pla Director consistirà en l'avaluació dels nostres actius, considerant les dependències existents entre ells i realitzant una valoració

3.2 Actius

La tipificació dels actius, es tant una informació documental d'interès com un criteri d'identificació d'amenaces potencials i salvaguardes apropiades a la naturalesa de l'actiu.

En un sistema d'informació trobem 2 coses essencials:

- La informació que s'utilitza
- Els serveis que es presten

Aquests dos actius essencials marquen els requisits de seguretat per a tots els demés components del sistema.

Dins de la informació que s'utilitza pot ser interessant considerar algunes característiques formals tals com si son de caràcter personal, amb requisits legals, o estan sotmesos a alguna classificació de seguretat, amb requisits normatius.

3.2.1 Actius Essencials

Com es comenta anteriorment, els actius essencials, marcaran els requisits de seguretat per als demés components; en el nostre cas, la organització conta amb dos actius essencials per al correcte desenvolupament del negoci:

Rebuda de Comandes: Acció que realitzen els clients, comprant un producte a la web.
Gestió de Comandes: Tramitació d'una comanda de les oficines a magatzem.

Sense aquests dos actius, la organització no podria funcionar correctament, es per això, que seran la base de la seguretat per a tots els demes elements del sistema.

La següent taula mostra els principals actius de la organització.

Àmbit	**Actius**
Actius essencials	*Rebuda de comandes.*
	Gestió comandes.
Instal·lacions	CPD(Sala de servidors)
	Oficines(plantes)
Hardware	Estacions de treball
	Servidors xarxa interna
	Servidors xarxa externa
Aplicació	Aplicació web
	Aplicació gestió comandes
	Aplicació comptabilitat
Serveis d'Informació	BB.DD. Aplicació Web
	BB.DD. Interna
Xarxa	Xarxa LAN
	Firewall
Serveis interns	*Testeig de noves versions de l'aplicació web*
	Accés al correu electrònic
	Accés als fitxers compartits
	Accés a internet per part dels usuaris.
	Gestió de comptes
	Captació de clients.
Serveis subcontractats	ADSL Connexió a internet
Equipament auxiliar	Aire Condicionat
Personal	Administrador de Sistemes
	Usuaris

3.3 Dependències

Els actius essencials són la informació i els serveis prestats; però aquests actius depenen d'altres actius com poden ser els equips, les comunicacions, les instal·lacions i les freqüentment oblidades persones que treballen en aquells.

Per això, apareix com a important el concepte de "dependències entre actius" o la mesura en que un actius superior es veuria afectat per un incident de seguretat en un actius inferior.

Es diu que un "actiu superior" depèn d'un "actiu inferior" quan la materialització d'una amenaça a l'actiu inferior, té com a conseqüència un perjudici sobre l'actiu superior.

3.3.1 Dependències dels Serveis Essencials

[Actius]Rebuda de comandes:

- Servidors Xarxa Externa
  - Aplicació Web
    - BBDD Aplicació Web
- ADSL

[Actius]Gestió de comandes:

- Servidors Xarxa Interna
  - Aplicació Gestió de Comandes
    - BBDD Interna
- Xarxa Local
- ADSL

3.3.2 Dependències dels Serveis Interns

[Actiu] Testeig de noves versions de l'aplicació web:

- Estacions de treball(usuaris)
- Servidors Xarxa Interna
- Xarxa LAN

[Actiu] Correu electrònic

- Accés a Internet d'usuaris
- Servidor xarxa Interna

[Actiu] Fitxers compartits

- Servidors Xarxa Interna
- Xarxa LAN

[Actiu] Accés a internet d'usuaris

- Connexió ADSL
- Firewall

[Actiu] Gestió de comptes

- Xarxa LAN

- Aplicació Comptabilitat
  - BBDD Interna
- Estacions de treball

[Actiu] Captació de clients
- Estacions de treball
- Accés a internet d'usuaris

[Actiu] Servidors Xarxa Interna
- CPD

[Actiu] Servidors Xarxa Externa
- CPD

[Actiu]Estacions de treball
- Oficines

[Actiu]Xaxa LAN
- Servidors Xarxa Interna.

3.4 Anàlisi de Riscos

Un cop ja es disposa d'un inventari dels actius de l'empresa i s'han establert les dependències entre ells es durà a terme l'anàlisi de riscos, començant per realitzar una valoració dels actius.

A l'Annex 1, trobem l'Anàlisi de Riscos de l'empresa XXX S.L.

3.4.1 Valoració dels actius

La valoració dels actius es una activitat fonamental en el procés d'Anàlisi de Riscos i es el procés per el qual es determinen les conseqüències d'un incident de seguretat sobre un actiu. La valoració d'un actiu es la mesura de les conseqüències de l'incident.

3.4.2 Identificació i valoració d'amenaces

Es la fase on es defineixen les amenaces a la que estan subjectes els diversos actius identificats i l'impacte que causaria sobre els mateixos la seva materialització.

S'utilitzen les amenaces usades en MAGERIT (en concret Llibre 2 "Catàleg d'elements" (Punt 5)).

Les amenaces estan classificades en els següents grans blocs:

- Desastres naturals
- D'origen industrial
- Error i fallades no intencionades
- Atacs intencionats

3.5 Dimensions de la Seguretat de la Informació

Tradicionalment, parlar de seguretat de la informació era referir-se als tres pilars bàsics:

• Confidencialitat[C]: només les persones autoritzades tenen accés a la informació sensible o privada.

• Integritat[I]: la informació i els mètodes de processament d'aquesta informació són exactes i complets, i no s'han de manipular sense autorització.

• Disponibilitat[D]: els usuaris que hi estan autoritzats poden accedir a la in-formació quan ho necessitin.

No obstant això, considerarem també altres dimensions de la seguretat, previstes per la mateixa legislació vigent:

• Autenticitat i no-repudi[A]: hi ha garantia de la identitat dels usuaris o processos que tracten la informació i de l'autoria d'una determinada acció.

• Traçabilitat[T]: és possible reproduir un històric o seqüència d'accions sobre un determinat procés i determinar qui ha estat l'autor de cada acció.

En l'Anàlisi de riscos s'assignarà un valor a cada dimensió de la seguretat dels actius, segons com es preveu que afectarà una amenaça.

3.6 Conclusions

Les principals amenaces que afecten als serveis de la capa de negoci de la organització(Recepció de comandes i Gestió de comandes) son tant errors com fallades no intencionades com atacs deliberats que podrien afectar la disponibilitat i la autenticitat dels usuaris en els serveis esmentats.

Cap destacar la quantitat d'amenaces a les que es vulnerable el servidor i el gran impacte que tindria en la organització la afectació del mateix. L'ús de privilegis d'accés no autoritzats i/o la difusió de software malintencionat, podria posar en perill la confidencialitat i la

integritat de la informació; d'altra banda, les amenaces d'origen natural o catàstrofes industrials, podrien posar en perill la disponibilitat de les instal·lacions, afectant d'aquesta manera als actius essencials, els quals depenen de les mateixes.

Fase 4: Auditoria i compliment de la ISO:IEC 27002:2005

A l'Annex 2, trobem l'Anàlisi dels controls ISO:IEC 27002:2005 per a l'empresa XXX S.L.

4.1 Introducció

L'objectiu d'aquesta fase del projecte és avaluar la maduresa de la seguretat pel que fa als 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.

4.2 Dominis de l'estàndard ISO 27002:2005

- 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

4.3 Avaluació de la maduresa

En aquest apartat, ens plantejarem millorar el compliment dels controls dels dominis de seguretat definits anteriorment. Analitzarem el compliment en quatre fases diferenciades:

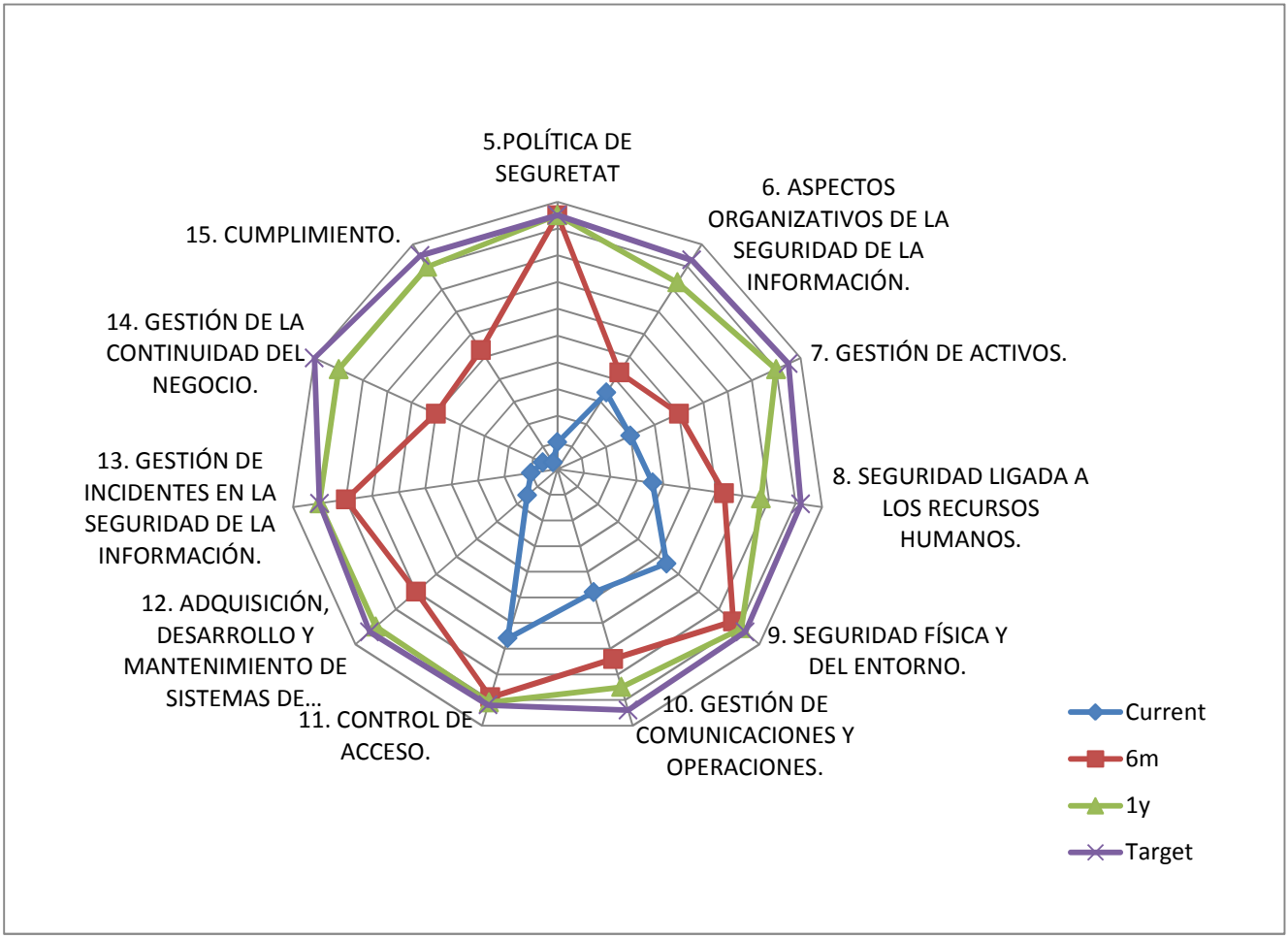
- Current: Estat actual de la seguretat
- 6m: Estat de la seguretat als 6 mesos.
- 1y: Estat de la seguretat al primer any.
- Target: Objectiu final, el tercer any des de la implantació.

L'estudi ha de fer 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 queden 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 Conclusions

El següent gràfic ens mostra d'una manera genèrica el nivell de compliment de cadascun dels dominis de seguretat en les quatre fases en que hem dividit el nostre projecte.



Es pot observar el baix compliment inicial dels controls ISO 27002:2005. Per tal de millorar el més ràpidament possible, es pretén crear una política de seguretat amb la màxima brevetat possible, ja que serà la base, el codi de conducta que seguiran els treballadors de l'empresa, i s'estima que la seva creació i seguiment hauran de ser molt avançats a la primera fase del projecte(6m).

La resta de controls, sofreixen un increment exponencial del seu compliment fins a arribar a assolir un nivell de maduresa adient per al bon desenvolupament de la organització.

Fase 5: Projectes de millora

5.1.Introducció

Arribats a aquest punt, coneixem ja l'estat de la seguretat en l'empresa i el nivell de compliment dels controls ISO. És el moment de plantejar projectes que millorin l'estat de la seguretat en l'organització.

5. Política de Seguretat

El principal objectiu serà la creació d'una política de Seguretat adient per a l'empresa, serà d'ús públic i marcarà les pautes a seguir per als treballadors de l'empresa. Amb la política definirem les bases del que serà el nostre SGSI.

La política mostrarà la implicació de la direcció en el sistema de gestió de seguretat de la informació i la signarà el director general de l'empresa.

Aquesta política s'aplicarà a curt termini amb la finalitat de realitzar les millores pertinents en la organització seguint uns criteris que vindran marcats per la mateixa.

L'objectiu final, a tres anys vista d'aquest projecte serà la obtenció d'una política estructurada i constantment en revisió adaptant-la a les necessitats de l'empresa.

A l' ANNEX "A" adjunta la Política de Segureta

6. Organització de la seguretat de la informació.

En aquest punt, es volen obtenir resultats amb la màxima brevetat possible, degut a que la implicació de la organització i la coordinació de la seguretat de la informació ens serviran com a directrius per als diferents controls de millora realitzats properament.

D'aquesta manera, es crearà un Comitè de Seguretat de la Informació, que serà l'encarregat d'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 i que supervisarà i aprovarà el desenvolupament del pla de continuïtat del negoci.

Aquest comitè contarà amb un Responsable de Seguretat de la Informació, juntament amb els responsables de les àrees de Màrqueting, Administració, Comercial, Recursos Humans, Comptabilitat i Tecnologies i Comunicacions.

Per a millorar els aspectes organitzatius de la seguretat de la informació, el comitè de la seguretat realitzarà reunions setmanals durant els primers sis mesos del pla, on l'ordre del dia serà debatre i comentar la millora i el compliment de les directrius de la organització interna[6.1].

Amb aquestes reunions setmanals es vol definir un procés en els sis primers mesos del pla (90% segons el model CCM). Un cop assolits els sis primers mesos, es continuaran realitzant reunions cada dues setmanes per tal de seguir amb un procés de constant millora que començarà pel que fa a la organització interna, i intentar aconseguir el mateix pel que fa els aspectes de la seguretat de la informació relacionat amb terceres parts[6.2].

L'objectiu final en aquest àmbit, serà la inclusió de la seguretat de la informació com a un punt diferenciat en els pressuposts de la organització, per tal que el comitè de Seguretat pogués gestionar els seus propis recursos.

7. Gestió d'actius

Amb la Política de Seguretat s'identifiquen, documenten i implementen regulacions envers l'ús adequat dels actius, queden definides també les directrius de classificació d'actius.

D'altra banda, degut al reduït nombre de persones amb les que consta la organització, mitjançant el correu electrònic corporatiu, es donarà ordre a tots els treballadors i/o directius de l'empresa de que documentin mitjançant un formulari web els actius que tenen en aquest moment a la seva disposició.

Amb aquesta base, el Comitè de Seguretat podrà començar a elaborar un inventari d'actius. També s'encarregaran d'assignar provisionalment actius al personal de l'empresa.

Durant els primers sis mesos, l'objectiu simplement serà la captació d'informació sobre els actius i la assignació provisional de diferents actius als treballadors.

L'objectiu a mitjà termini (un any) serà que tots els actius deuran ser justificats i tenir-hi assignat un propietari. Al propietari de l'actiu se li assignarà la responsabilitat de manteniment dels controls adients.

Amb aquesta informació, el departament de sistemes elaborarà una base de dades mitjançant Microsoft Access amb les taules corresponents als criteris anteriors.

Aquest procés tindrà com a objectiu final tenir un inventari d'actius gestionat i mesurable, podent consultar qualsevol actiu mitjançant consultes a la base de dades de Microsoft Access.

8. Seguretat lligada als recursos humans

Els processos de selecció dels candidats variaran segons el lloc per al que volen ser contractats, depenent en gran mesura de la classificació de seguretat d'aquella informació a la que tindran accés. En una primera fase, es treballarà conjuntament amb RRHH per a conscienciar de la se va importància. L'objectiu final, serà assolir un procés documentat amb qüestionaris i mètodes de recerca adients per a cada situació.

En el cas que es necessiti informar a tot el personal d'alguna debilitat amb respecte a la seguretat, s'utilitzarà com a primera instància el correu electrònic intern i si el cas fos excepcional, es convocaria una reunió en la qual intervindrà el Comitè de Seguretat juntament amb el personal de direcció necessari. Durant la primera fase, es pretendrà donar a conèixer als treballadors de l'empresa la situació actual, per tal de poder definir un procés documentat i comunicat on hi participin tots els individus

En referència al cessament de la feina o canvi d'ocupació, durant la primera fase es vol assolir un procés definit.

Per a definir aquest procés:

- S'assignarà al departament de RRHH la responsabilitat de comunicar a l'equip pertinent la revocació o modificació de drets d'un usuari. Durant la primera fase, es realitzarà una reunió amb els caps de cada divisió i el Comitè de seguretat per a tractar aquest tema.

- S'afegirà als contractes d'alta una clàusula que indiqui explícitament la obligació d'una immediata devolució dels actius que pertanyen a l'empresa abans d'abandonar la mateixa.

9. Seguretat física i ambiental

Segons els resultats obtinguts en l'Anàlisi de Riscos i la impossibilitat de millorar el perímetre de la seguretat física, ja que queda fora de l'abast del SGSI degut a que a l'edifici hi conviuen tres empreses més, es millorarà la seguretat en els controls físics d'entrada.

S'implantarà a mig termini un control d'accés a les dues plantes de l'empresa mitjançant les targetes utilitzades per entrar a l'edifici. D'aquesta manera evitarem la possibilitat que personal autoritzat a entrar a l'edifici a través de les altes dues empreses que cohabiten a l'edifici pugin accedir a les dependències de la organització.

Pel que fa a la CPD, un actiu essencial en els processos crítics de la organització, es canviarà l'actual sistema d'entrada amb clau per un sistema d'entrada mitjançant la mateixa targeta d'accés a la organització, que haurà de ser proveïda dels permisos adients i que s'haurà de validar a la porta, juntament amb la introducció d'un codi personal i intransferible.

Els codis s'hauran de canviar cada trimestre i a les reunions del Comitè de Seguretat es validaran les persones autoritzades per a l'accés al CPD.

10. Gestió de comunicacions i operacions

Es documentaran i mantindran actualitzats els procediments operatius i els seus canvis seran autoritzats per el responsable TIC.

El responsable de l'àrea d'informàtica serà l'encarregat d'implementar els canvis operacionals i de comunicacions, prèvia una justificació que expliqui els motius i com millorarà en la productivitat de la organització

Aquests procediments de control, contemplaran els següents punts:

- Identificació i registre de canvis significatius
- Avaluació del possible impacte dels canvis
- Aprovació formal dels canvis proposats
- Planificació del procés de canvi
- Prova del nou escenari
- Comunicació de detalls de canvis a les persones pertinents
- Identificació de responsabilitats

El responsable de la Seguretat de la Informació disposarà i controlarà la realització de les copies de seguretat. Els sistemes de backup deuran provar-se periòdicament als entorns de prova, per assegurar que compleixen els requeriments del pla de continuïtat de les activitats de la organització.

Es seguirà el següent procediment:

- Emmagatzemar en una ubicació remota les copies recents de la informació, juntament amb els procediments documentats de restauració; es guardaran a una distància suficient com per a evitar danys provinents d'un desastre en la zona principal.
- Assignar als backups un nivell de protecció física i ambiental segons les normes aplicades al lloc principal.
- Verificar i provar periòdicament els procediments de restauració garantint així la seva eficàcia i compliment.

La organització es protegirà amb cadenats per a les computadores portàtils per a evitar que siguin robades. Es compraran els cadenats i es cediran juntament amb el portàtil.

11. Control d'accés

Es crearà una norma sobre l'ús de les contrasenyes que serà difosa als treballadors de la organització mitjançant el correu electrònic. Aquesta norma es crearà durant la primera fase del SGSI.

ANNEX B (Normativa contrasenyes)

12. Adquisició, desenvolupament i manteniment de Sistemes d'Informació

Es definirà un procés a mig termini per a controlar canvis en la adquisició, desenvolupament i manteniment dels sistemes d'informació

- Sol·licitud del canvi al responsable de la unitat.
- Aprovació del canvi.
- Documentació del canvi
- Proves i presentació
- Implementació
- Documentació del control de canvis: Els canvis que deuran ser documentats seran
    - Instal·lació de nous PS
    - Instal·lació de noves aplicacions
    - Implementació de diferents configuracions
    - Instal·lació d'actualitzacions
    - Polítiques o procediments actualitzats
    - Nous dispositius connectats a la xarxa.

Per a evitar que els usuaris pugin modificar sense autorització prèvia qualsevol tipus de software, les contes dels empleats en el domini no tindran permisos per a realitzar ninguna d'aquestes activitats, així com tampoc podran instal·lar qualsevol tipus de software ni esborrar-lo sense una sol·licitud prèvia al administrador de la xarxa(Responsable TIC) i el responsable de l'àrea pertinent.

13. Gestió d'incidents

Actualment no existeix cap mecanisme per a notificar esdeveniments relacionats amb la seguretat de la Informació. A curt termini, es conscienciarà als treballadors de la necessitat de la comunicació d'aquests incidents, mitjançant la política de seguretat i les ja citades reunions i informacions via correu electrònic.

L'objectiu en la segona fase serà implementar les incidències i millores de la seguretat de la informació a la eina ITSM utilitzada per la organització. Aquesta millora serà realitzada per els desenvolupadors de l'empresa i s'utilitzarà tant per a millores com per a defectes i propostes, aquestes, seran assignades directament al Responsable de seguretat. D'aquesta manera s'aconseguirà recopilar evidències trobades pel personal i es conscienciarà als departaments de la importància de la Seguretat

14. Gestió de continuïtat del negoci.

Els responsables de cada àrea determinaran les aplicacions crítiques de les mateixes i desenvoluparan procediments regulars per a mantenir recolzats contínuament els processos crítics de cadascuna. El pla de contingència de cada procés considerarà com a mínim:

- La administració dels recursos crítics, en cas de ser necessària la implementació del pla de contingència.
- Identificació dels riscos. Cada risc deurà ser identificat amb quins passos serien necessaris per a detenir-lo,
- Documentar l'impacte d'una pèrdua estesa a les funcions del negoci.
- Deu ser una pla fàcil d'utilitzar i fàcil de mantenir per tots els membres de la organització

L'objectiu a curt termini serà aconseguir conscienciar els treballadors, amb la ajuda de la creació de la Política de Seguretat i la implicació des de la direcció en matèria de la seguretat de la informació, per tal que en el termini d'un any pugui existir un procés definit on hi estigui implicada la organització.

Un cop documentat tot el procés, es duran a terme simulacres per tal de pel Comitè de Seguretat per tal de millorar contínuament el procés.

Els resultats del simulacre seran de l'ordre del dia de les reunions del Comitè de Seguretat.

15. Compliment

Es redactarà una conducta que deuran complir tots els empleats , la copia signat del compromís serà retinguda per l'empresa. A través del Compromís de Confidencialitat es deurà advertir a l'empleat que determinades activitats podran ser objecte de control i monitoratge. Es detallaran aquestes activitats a fi de no violar la privacitat de l'empleat.

Annex 1. Anàlisi de Riscos

1.1 Valoració d'actius.

Valoració numèrica de les dimensions de seguretat dels actius en funció del dany que podria causar a la organització el fet que fossin compromesos.

Àmbit	**Actius**	**Valoració**	**Aspectes Crítics**				
			A	**C**	**I**	**D**	**T**
Actius essencials	*Rebuda de comandes.*	Molt Alta	X	X	X	X	X
	Gestió comandes(magatzem)	Alta	X	X	X	X	X
Instal·lacions	CPD	Molt Alta	6	8	8	10	8
	Oficines(plantes)	Mitjana	5	6	7	8	7
Hardware	Estacions de treball	Mitjana	5	6	7	8	7
	Servidors xarxa interna	Mitjana	5	6	7	8	7
	Servidors xarxa externa	Molt Alta	6	8	8	10	8
Aplicació	Aplicació web	Molt Alta	6	8	8	10	8
	Aplicació gestió comandes	Alta	5	6	7	8	7
	Aplicació comptabilitat	Mitjana	5	6	7	8	7
Serveis d'Informació	BB.DD. Aplicació Web	Molt Alta	6	8	8	10	8
	BB.DD. Interna	Alta	5	6	7	8	7
Xarxa	Xarxa LAN	Mitjana	5	6	7	8	7
	Firewall	Mitjana	X	X	X	7	X
Serveis interns	*Testeig de noves versions de l'aplicació web*	Mitjana	3	X	X	3	3
	Correu electrònic	Alta	8	X	X	3	8
	Fitxers compartits	Mitjana	9	X	X	5	9
	Accés a internet d'usuaris.	Baixa	3	X	X	3	3
	Gestió de comptes	Mitjana	8	X	X	5	8
	Captació de clients.	Baixa	X	X	X	3	X
Serveis subcontractats	ADSL Connexió a internet	Molt Alta	X	X	X	10	X
Equipament	Aire Condicionat	Alta	X	X	X	10	X

auxiliar							
Personal	Administrador de Sistemes	Alta	X	X	X	9	X
	Usuaris	Mitjana	X	X	X	7	X

1.1.1 Criteri de Valoració

En la següent taula observem els criteris que es segueixen a l'hora de valorar les dimensions de seguretat d'un actiu.

VALOR	**CRITERI**
10	Dany molt greu a la organització
7-9	Dany greu a la organització
4-6	Dany important a la organització
1-3	Dany menor a la organització
0	Irrellevant per la organització
X	No afecta

1.2 Anàlisi d'Amenaces

En aquesta taula es mostra la freqüència amb la que es pot produir una amenaça, així com el seu impacte per al procés de Recepció de Comandes, així com als actius dels qual depèn aquest procés.

Actiu	**Freqüència**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[Essencials]Recepció de comandes						
[HARDWARE]Servidors Xarxa Externa		100%	50 %	50 %	100 %	100 %
[Aplicació]Aplicació Web		100%	50 %	50 %	100 %	100 %
[Serveis d'Informació] BBDD Aplicació Web		100%	50 %	50 %	100 %	100 %
[Serveis subcontractats] ADSL]		100%	50 %	50 %	100 %	100 %
[I] De origen industrial						
[I.1] Fuego	MPF				100 %	
[I.2] Daños por agua	MPF				100	

					%	
[I.6] Corte del suministro eléctrico	F				100 %	
[I.7] Condiciones inadecuadas de temperatura o humedad	PF				60%	
[I.8] Fallo de servicios de comunicaciones	F				100 %	
[I.10] Degradación de los soportes de almacenamiento de la información	MPF				50%	
[E] Errores y fallos no intencionados						
[E.1] Errores de los usuarios	EF		1%	1%	1%	
[E.2] Errores del administrador	F	10%	10 %	20 %	20%	20%
[E.3] Errores de monitorización *(log)*	MF					40%
[E.4] Errores de configuración	F	60%	10 %	10 %	60%	60%
[E.14] Escapes de información	PF		20 %			
[E.15] Alteración accidental de la información	PF			1%		
[E.18] Destrucción de información	PF				1%	
[E.20] Vulnerabilidades de los programas (software)	F				5%	
[E.21] Errores de mantenimiento / actualización de programas (software)	PF			10 %	10%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PF			10 %	10%	
[E.24] Caída del sistema por agotamiento de	MPF				60%	

recursos						
[E.25] Pérdida de equipos	MPF				60%	
[E.28] Indisponibilidad del personal	MPF				1%	
[A] Ataques intencionados						
[A.3] Manipulación de los registros de actividad (log)	PF					100 %
[A.4] Manipulación de la configuración	PF	100%	50 %	10 %	50%	100 %
[A.5] Suplantación de la identidad del usuario	PF	50%	50 %	10 %	100 %	
[A.11] Acceso no autorizado	F	50%	50 %	10 %	100 %	
[A.24] Denegación de servicio	F				100 %	
[A.26] Ataque destructivo	F				100 %	
[A.28] Indisponibilidad del personal	F				10%	
[A.30] Ingeniería social (picaresca)	F	50%		50 %		

En aquesta taula es mostra la freqüència amb la que es pot produir una amenaça, així com el seu impacte per al procés de Gestió de Comandes, així com als actius dels qual depèn aquest procés.

Actiu	**Freqüència ******	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[Essencials]Gestió de comandes						
[HARDWARE]Servidors Xarxa Interna		100 %	100 %	50 %	100 %	100 %
[Aplicació]Aplicació Gestió de comandes		100 %	100 %	50 %	100 %	100 %
[Serveis d'Informació] BBDDInterna		100 %	100 %	50 %	100 %	100 %
[Serveis subcontractats] ADSL]		100 %	100 %	50 %	100 %	100 %

[Xarxes]Xarxa LAN		100 %	100 %	50 %	100 %	100 %
[I] De origen industrial						
[I.1] Fuego	MPF				100 %	
[I.2] Daños por agua	MPF				100 %	
[I.6] Corte del suministro eléctrico	F				100 %	
[I.7] Condiciones inadecuadas de temperatura o humedad	PF				60%	
[I.8] Fallo de servicios de comunicaciones	F				100 %	
[I.10] Degradación de los soportes de almacenamiento de la información	MPF				50%	
[E] Errores y fallos no intencionados						
[E.1] Errores de los usuarios	EF		1%	1%	1%	
[E.2] Errores del administrador	F	10%	10%	20 %	20%	20%
[E.3] Errores de monitorización *(log)*	MF					60%
[E.4] Errores de configuración	F	50%	10%	10 %	50%	50%
[E.14] Escapes de información	PF		20%			
[E.15] Alteración accidental de la información	PF			1%		
[E.18] Destrucción de información	PF				1%	
[E.20] Vulnerabilidades de los programas (software)	F				5%	
[E.21] Errores de mantenimiento / actualización de programas (software)	PF			10 %	10%	

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PF			10 %	10%	
[E.24] Caída del sistema por agotamiento de recursos	MPF				60%	
[E.25] Pérdida de equipos	MPF				60%	
[E.28] Indisponibilidad del personal	MPF				1%	
[A] Ataques intencionados						
[A.3] Manipulación de los registros de actividad (log)	PF					100 %
[A.4] Manipulación de la configuración	PF	100 %	50%	10 %	50%	100 %
[A.5] Suplantación de la identidad del usuario	PF	50%	50%	10 %	100 %	
[A.11] Acceso no autorizado	F	50%	50%	10 %	100 %	
[A.19] Divulgación de información	MPF		100 %			
[A.24] Denegación de servicio	F				100 %	
[A.26] Ataque destructivo	F				100 %	
[A.28] Indisponibilidad del personal	F				10%	
[A.30] Ingeniería social (picaresca)	F	50%		50 %		

1.2.1 Criteris de Freqüència

Vulnerabilitat	sigles	Rang	Valor
Extremadament freqüent	EF	1 vegada al dia	365/365=1
Molt freqüent	MF	1 vegada per setmana	52/365=0.142
Freqüent	F	1 vegada al mes	12/365=0.033
Poc freqüent	PF	1 vegada cada tres mesos	4/365=0.011
Molt poc freqüent	MPF	1 vegada a l'any o menys	1/365=0.003

Annex 2 - Controls ISO: Estat inicial i objectiu.

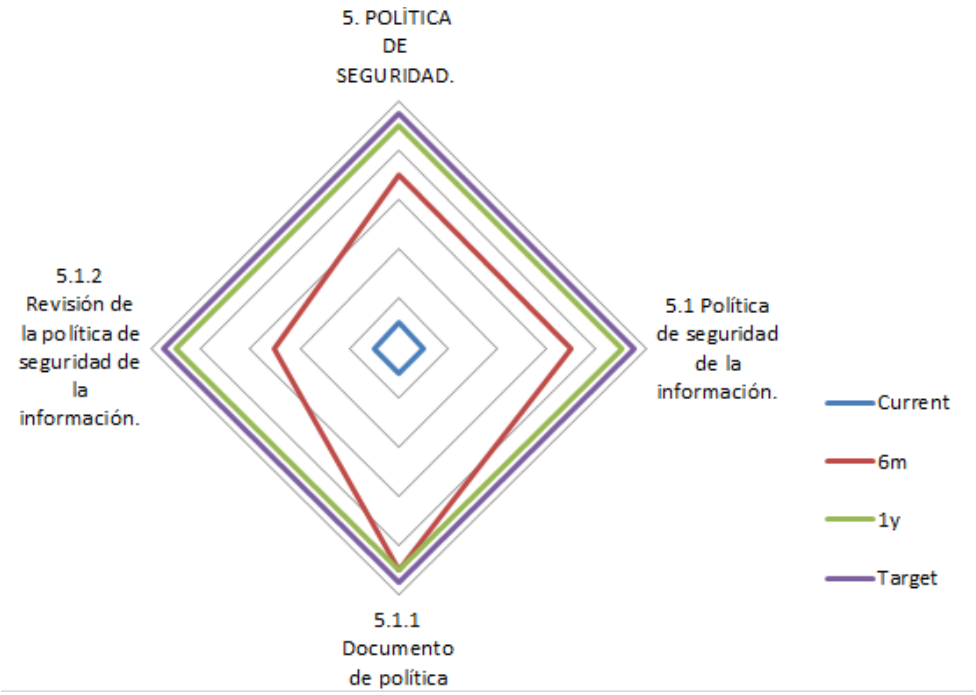
5. Política de seguretat

CONTROL	Current	6m	1y	Target
5. POLÍTICA DE SEGURIDAD.	**10%**	**70%**	**90%**	**95%**
5.1 Política de seguridad de la información.	**10%**	**70%**	**90%**	**95%**
5.1.1 Documento de política de seguridad de la información.	10%	90%	90%	95%
5.1.2 Revisión de la política de seguridad de la información.	10%	50%	90%	95%

Actualment no trobem definida una política de seguretat com a tal[5.1.1][5.1.2], es podria dir que la trobem en un estat inicial, ja que trobem definits certs processos no documentats que el seu compliment recau en el personal de l'empresa.

L'objectiu en aquest cas, es crear una política perfectament definida i actualitzada constantment, amb l'objectiu d'implicar a tota la organització i definir unes pautes adients per a desenvolupament de la mateixa i amb una constant actualització.

Aquest objectiu es vol assolir en la primera de les fases, ja que esdevindrà la base de molts controls i codis de conducta, que s'aplicaran en diferents controls.



6. Aspectes organitzatius de la seguretat de la inforamació.

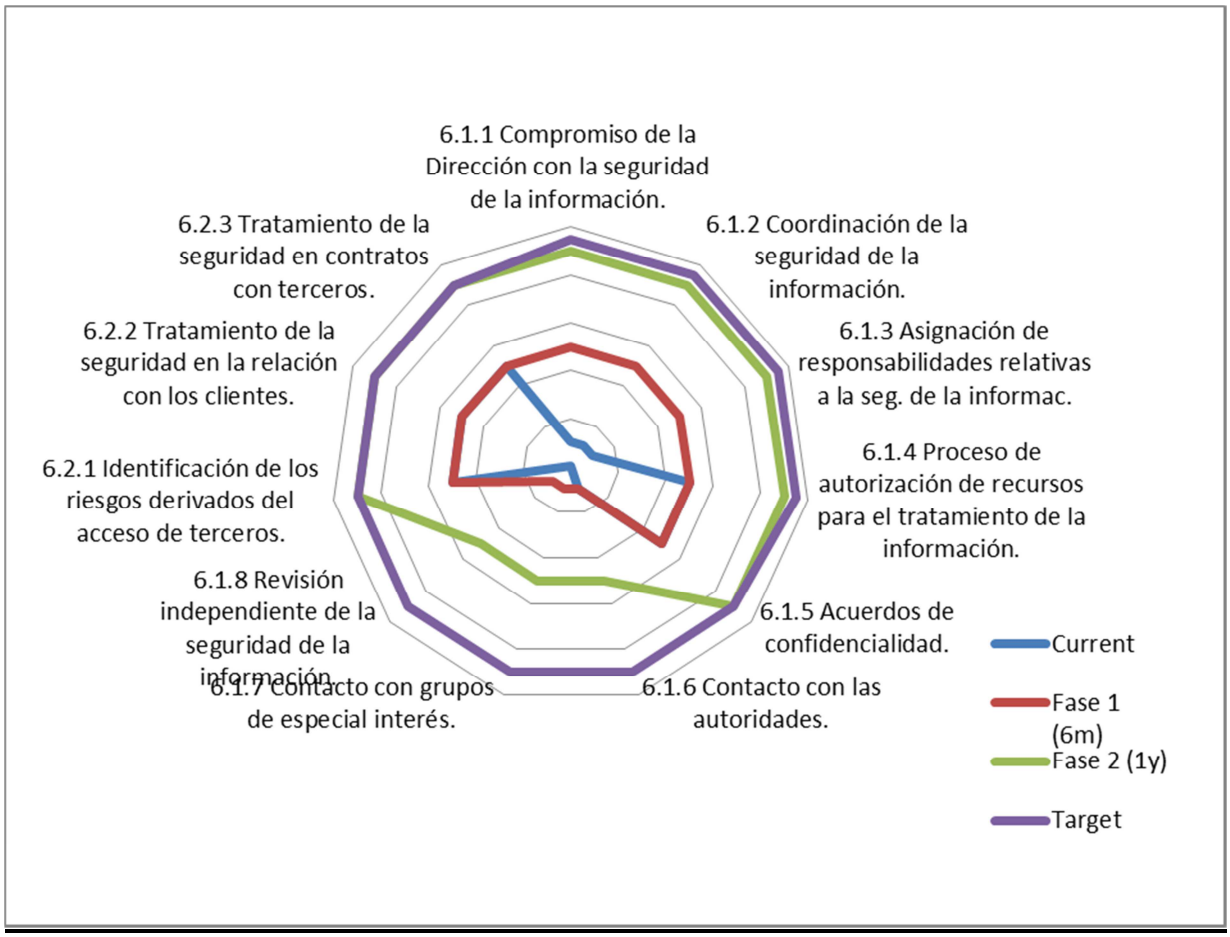
CONTROL	Current	6m	1y	Target
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	**34%**	**43%**	**83%**	**93%**
6.1 Organización interna.	**18%**	**35%**	**75%**	**93%**
6.1.1 Compromiso de la Dirección con la seguridad de la información.	10%	50%	90%	95%
6.1.2 Coordinación de la seguridad de la información.	10%	50%	90%	95%
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.	10%	50%	90%	95%
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	50%	50%	90%	95%
6.1.5 Acuerdos de confidencialidad.	50%	50%	90%	90%
6.1.6 Contacto con las autoridades.	10%	10%	50%	90%
6.1.7 Contacto con grupos de especial interés.	0%	10%	50%	90%
6.1.8 Revisión independiente de la seguridad de la información.	0%	10%	50%	90%
6.2 Terceros.	**50%**	**50%**	**50%**	**50%**
6.2.1 Identificación de los riesgos derivados del acceso de terceros.	50%	50%	90%	90%
6.2.2 Tratamiento de la seguridad en la relación con los clientes.	50%	50%	90%	90%
6.2.3 Tratamiento de la seguridad en contratos con terceros.	50%	50%	90%	90%

Com es pot veure en l'estat inicial de la seguretat, trobem una organització en la que la direcció no té un compromís[6.1.1] amb la seguretat de la informació més enllà del que es pot considerar de sentit comú, sense cap documentació explícita ni cap procés definit . Es per això que catalogarem el compromís de la direcció com a Inicial, amb la finalitat de millorar-lo, assegurant un compromís de la mateixa a través de la Política de Seguretat, creada prèviament. De la mateixa manera considerem la coordinació de la seguretat de la informació[6.1.2] i la assignació de responsabilitats.

Aquest compromís esdevindrà durant la primera fase, on també s' assignaran responsabilitats[6.1.3] i es marcaran unes pautes en aquest aspecte per tal de poder exercir un control més gran sobre els diferents processos de la organització. Posteriorment es vol avançar

fins a un control optimitzats en algun dels aspectes organitzatius de la seguretat de la informació.

Respecte als riscos derivats de l'accés de tercers[6.2], ens trobem en un punt inicial on els riscos són coneguts i controlats però no existeix una documentació a seguir. durant la primera fase no es vol assolir cap millora, no obstant durant la segona fase, es vol assolir un procés definit, que pugi ser conegut per els empleats de l'empresa.



7. Gestió d'actius

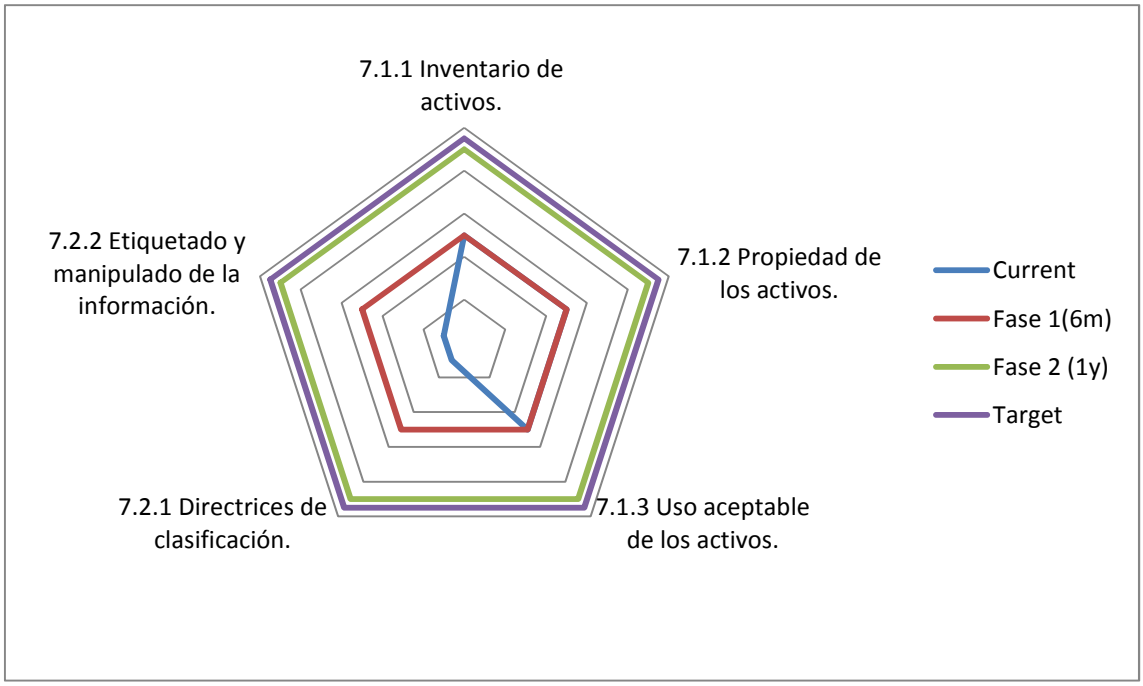
CONTROL	Current	6m	1y	Target
7. GESTIÓN DE ACTIVOS.	**30%**	**50%**	**90%**	**95%**
7.1 Responsabilidad sobre los activos.	**50%**	**50%**	**90%**	**95%**
7.1.1 Inventario de activos.	50%	50%	90%	95%
7.1.2 Propiedad de los activos.	50%	50%	90%	95%
7.1.3 Uso aceptable de los activos.	50%	50%	90%	95%
7.2 Clasificación de la información.	**10%**	**50%**	**90%**	**95%**

7.2.1 Directrices de clasificación.	10%	50%	90%	95%
7.2.2 Etiquetado y manipulado de la información.	10%	50%	90%	95%

Com es comenta en l'estat inicial de la seguretat, trobem un inventari[7.1.1] actualitzat mensualment, que contempla funcionalitat i importància de l'actiu[7.2.1], no obstant això, no segueix unes directrius prèviament definides, si no que és el propi treballador que realitza l'inventari el que qualifica d'una manera més o menys important l'actiu, etiquetant-los[7.2.2] amb un codi d'etiquetes conegut pels membres del seu departament, un codi que no està documentat i és difícilment interpretable per d'altres usuaris. L'inventari s'actualitza mensualment i tot i saber a qui pertany o té assignat un actiu[7.1.2] podríem tenir informació errònia durant un període important de temps.

D'altra banda no trobem cap regulació per a l'ús correcte dels actius[7.1.3], no obstant, els treballadors són conscients de la importància del bon ús dels mateixos per al correcte funcionament de la organització.

En aquest apartat, ens fixem l'objectiu d'establir unes polítiques a seguir durant la primera fase a l'hora d'inventariar els actius, implicant a la direcció de l'empresa, i accessibles als demés treballadors per tal que l'inventari sigui fàcilment intel·ligible per tothom i no es depengui en abundància dels coneixements del treballador a l'hora d'utilitzar aquest inventari, alhora s'assignaran responsabilitats



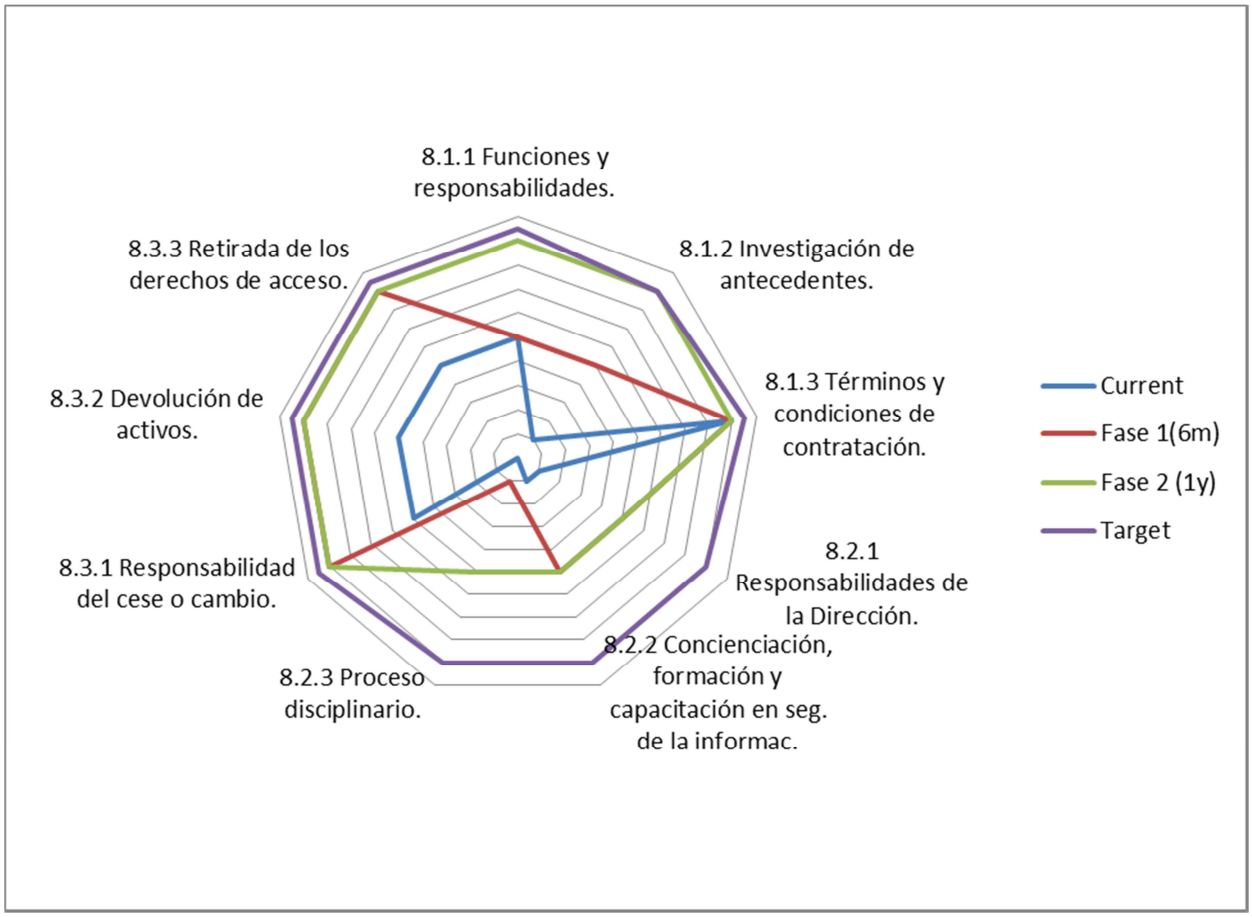
8. Seguretat lligada als Recursos Humans.

CONTROL	Current	6m	1y	Target
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**36%**	**63%**	**77%**	**92%**
8.1 Antes del empleo.	**50%**	**63%**	**90%**	**91%**
8.1.1 Funciones y responsabilidades.	50%	50%	90%	95%
8.1.2 Investigación de antecedentes.	10%	50%	90%	90%
8.1.3 Términos y condiciones de contratación.	90%	90%	90%	95%
8.2 Durante el empleo.	**7%**	**36%**	**50%**	**90%**
8.2.1 Responsabilidades de la Dirección.	10%	50%	50%	90%
8.2.2 Concienciación, formación y capacitación en seg. de la informac.	10%	50%	50%	90%
8.2.3 Proceso disciplinario.	0%	10%	50%	90%
8.3 Cese del empleo o cambio de puesto de trabajo.	**50%**	**90%**	**90%**	**95%**
8.3.1 Responsabilidad del cese o cambio.	50%	90%	90%	95%
8.3.2 Devolución de activos.	50%	90%	90%	95%
8.3.3 Retirada de los derechos de acceso.	50%	90%	90%	95%

Com es comenta en l'estat inicial de la seguretat, un cop es realitza una contractació, ja sigui l'alta d'un empleat com d'una altra empresa, es signen unes polítiques[8.1.3] de confidencialitat i no divulgació, que després de revisar, trobem que son adients. No obstant, aquestes documents no contemplen les funcions i responsabilitats que els empleats[8.1.1] o empreses han de seguir en concordança a la política de seguretat, degut a la absència de la mateixa.
Aquest procés millorarà un cop creada la Política de Seguretat, i aquests documents s'adaptaran a la nova política(primera fase)
D'altra banda, l'empresa no investiga en particular a les persones que seran contractades posteriorment[8.1.2], apartat, es millorarà durant la primera fase, instruint a les persones encarregades; durant la segona fase, es crearà un procés definit del mateix.

Un cop contractades les persones són informades[8.2.2] mitjançant uns documents de conscienciació, formació i capacitació en la seguretat de la informació. No obstant, aquests documents no són el suficientment detallats per a fer entendre la importància de la seguretat de la informació.
Es pretén fer una revisió dels següents documents implicant a la Direcció de l'empresa, [8.2.2], que en aquests moments no hi participa activament, de la mateixa manera que es vol implantar un procés disciplinari(avui en dia inexistent)[8.2.3] per tal de incrementar el compliment de les responsabilitats. Tot això es realitzarà durant la primera fase del procés, evolucionant fins a un procés optimitzat com a objectiu final.

Respecte a la sortida d'un treballador o al seu canvi de lloc de treball, l'empresa no té definides unes polítiques a seguir. La responsabilitat[8.3.1] recau en el superior immediat de la persona en qüestió. Pel que fa a la revocació de permisos i a la devolució d'actius[8.3.2][8.3.3], si que es un procés que es té molt en compte i es realitza constantment, però no està documentat, i tampoc especificat en les polítiques de contractació, fet pel qual, s'hauria d'afegir en els termes i condicions. Durant la primera fase es definirà un procés i s'anirà millorant fins a optimitzar-lo.



9. Seguretat física i de l'entorn.

CONTROL	Current	6m	1y	Target
9. SEGURIDAD FÍSICA Y DEL ENTORNO.	**54%**	**87%**	**91%**	**93%**
9.1 Áreas seguras.	**57%**	**83%**	**91%**	**95%**
9.1.1 Perímetro de seguridad física.	95%	95%	95%	95%
9.1.2 Controles físicos de entrada.	50%	90%	90%	95%
9.1.3 Seguridad de oficinas, despachos e instalaciones.	50%	90%	90%	95%
9.1.4 Protección contra las amenazas externas y de origen ambiental.	50%	90%	90%	95%
9.1.5 Trabajo en áreas seguras.	10%	50%	90%	95%
9.1.6 Áreas de acceso público y de carga y descarga.	NA	NA	NA	NA
9.2 Seguridad de los equipos.	**50%**	**90%**	**90%**	**90%**
9.2.1 Emplazamiento y protección de equipos.	50%	90%	90%	90%
9.2.2 Instalaciones de suministro.	50%	90%	90%	90%
9.2.3 Seguridad del cableado.	50%	90%	90%	90%
9.2.4 Mantenimiento de los equipos.	50%	90%	90%	90%
9.2.5 Seguridad de los equipos fuera de las instalaciones.	50%	90%	90%	90%

9.2.6 Reutilización o retirada segura de equipos.	50%	90%	90%	90%
9.2.7 Retirada de materiales propiedad de l'empresa.	50%	90%	90%	90%

Com es pot veure en l'estat inicial, l'accés a l'empresa [9.1.1] es realitza mitjançant targetes de banda magnètica, personals i intransferibles que serveixen per accedir a l'edifici. És un procés amb un alt nivell de compliment, pel que no es considera realitzar cap millora sobre ell. A més, a l'edifici hi poden accedir treballadors d'altres empreses, per la qual cosa no dependria exclusivament de l'empresa.

D'altra banda, l'accés a la sala de servidors es realitza mitjançant una clau que tenen els responsables d'aquesta àrea[9.1.2], aquest mecanisme no requereix cap identificació personal per a realitzar l'accés, això no està documentat, , no obstant no és un procés que es decideixi millorar.

Un cop a l'edifici, no trobem cap impediment en accedir a les oficines i instal·lacions del personal o els recursos no protegits de la planta[9.1.3], un aspecte a millorar considerablement durant la primera fase, degut a les facilitats que això comporta a una fuita d'informació. Una bona manera de millorar aquest aspecte seria amb la creació d'unes targetes diferents per accedir a les oficines.

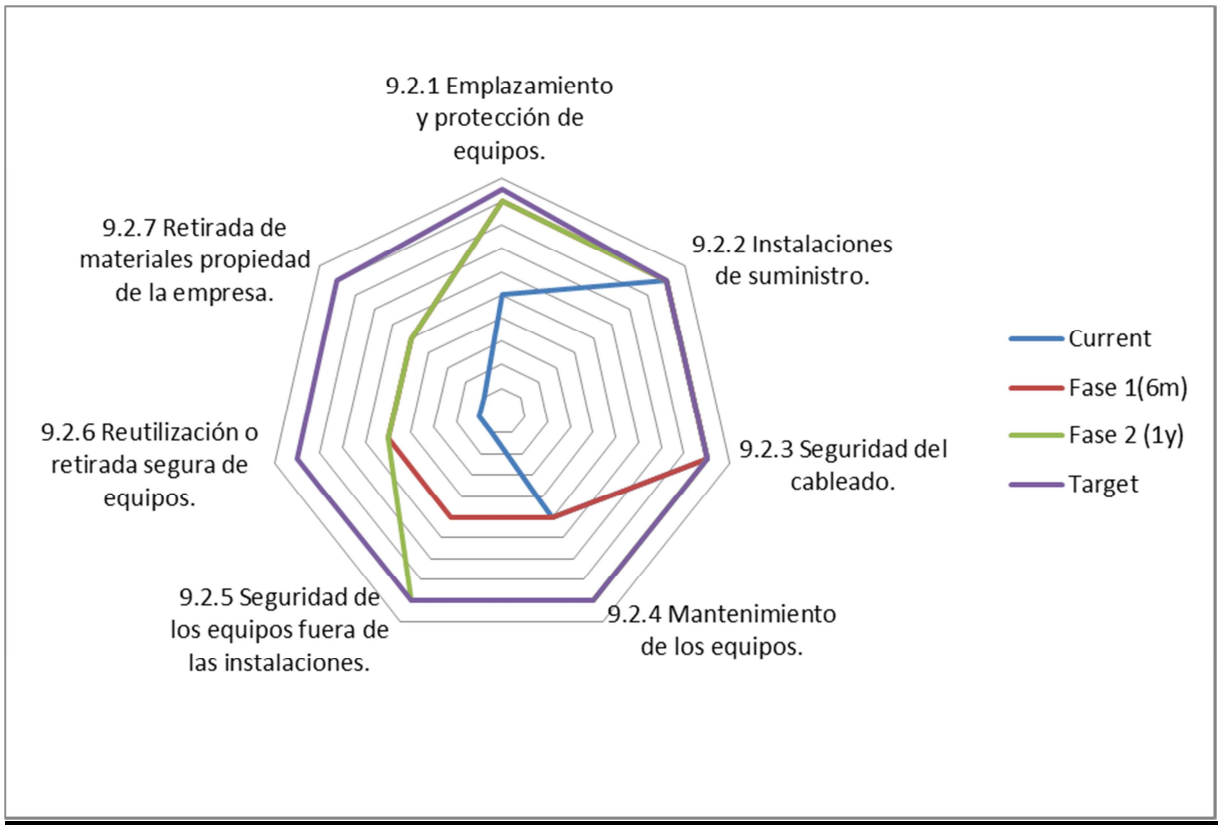
Respecte a les amenaces externes i d'origen ambiental[9.1.4] , no hi ha una política definida que abraci totes les possibilitats, però és un procés que podríem catalogar de reproduïble.

No trobem documentades cap pauta de comportament per a treballar en els espais segurs.[9.1.5]. En una primera fase, es vol fer saber als empleats la importància de complir un seguit de normes, per a poder definir un procés en les fases següents.

Les àrees de càrrega i descàrrega[9.1.6] es troben a la recepció de l'edifici, amb la qual cosa s'evita l'entrada de personal no autoritzat a l'interior, no obstant, aquesta política d'accés és regulada per l'empresa de seguretat que gestiona l'edifici.

Pel que fa a la seguretat en els equips, el CPD si que conta amb un SAI per a prevenir possibles problemes[9.2.2], no obstant, els ordinadors de sobretaula no en disposen. El cablejat[9.2.3] i el manteniment dels equips[9.2.4] queden a càrrec de cada individu.

Un cop es volen reutilitzar[9.2.6] o retirar[9.2.7] equips o materials propietat de l'empresa, es fa sota la supervisió de l'equip de sistemes, però no existeix un procés definit per a fer-ho.



10. Gestió de comunicacions i operacions

CONTROL	Current	6m	1y	Target
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	**48%**	**74%**	**85%**	**94%**
10.1 Responsabilidades y procedimientos de operación.	**58%**	**70%**	**90%**	**95%**
10.1.1 Documentación de los procedimientos de operación.	0%	50%	90%	95%
10.1.2 Gestión de cambios.	50%	50%	90%	95%
10.1.3 Segregación de tareas.	90%	90%	90%	95%
10.1.4 Separación de los recursos de desarrollo, prueba y operación.	90%	90%	90%	95%
10.2 Gestión de la provisión de servicios por terceros.	**50%**	**50%**	**50%**	**90%**
10.2.1 Provisión de servicios.	50%	50%	50%	90%
10.2.2 Supervisión y revisión de los servicios prestados por terceros.	50%	50%	50%	90%

10.2.3 Gestión del cambio en los servicios prestados por terceros.	50%	50%	50%	90%
10.3 Planificación y aceptación del sistema.	**10%**	**50%**	**50%**	**90%**
10.3.1 Gestión de capacidades.	10%	50%	50%	90%
10.3.2 Aceptación del sistema.	10%	50%	50%	90%
10.4 Protección contra el código malicioso y descargable.	**90%**	**95%**	**95%**	**95%**
10.4.1 Controles contra el código malicioso.	90%	95%	95%	95%
10.4.2 Controles contra el código descargado en el cliente.	90%	95%	95%	95%
10.5 Copias de seguridad.	**50%**	**90%**	**95%**	**100%**
10.5.1 Copias de seguridad de la información.	50%	90%	95%	100%
10.6 Gestión de la seguridad de las redes.	**50%**	**90%**	**95%**	**100%**
10.6.1 Controles de red.	90%	90%	95%	100%
10.6.2 Seguridad de los servicios de red.	10%	90%	95%	100%
10.7 Manipulación de los soportes.	**20%**	**50%**	**90%**	**90%**
10.7.1 Gestión de soportes extraíbles.	10%	50%	90%	90%
10.7.2 Retirada de soportes.	10%	50%	90%	90%
10.7.3 Procedimientos de manipulación de la información.	10%	50%	90%	90%
10.7.4 Seguridad de la documentación del sistema.	50%	50%	90%	90%
10.8 Intercambio de información.	**10%**	**58%**	**90%**	**90%**
10.8.1 Políticas y procedimientos de intercambio de información.	10%	50%	90%	90%
10.8.2 Acuerdos de intercambio.	10%	50%	90%	90%
10.8.3 Soportes físicos en tránsito.	10%	90%	90%	90%
10.8.4 Mensajería electrónica.	10%	50%	90%	90%
10.8.5 Sistemas de información empresariales.	10%	50%	90%	90%
10.9 Servicios de comercio electrónico.	**90%**	**95%**	**100%**	**100%**
10.9.1 Comercio electrónico.	90%	95%	100%	100%
10.9.2 Transacciones en línea.	90%	95%	100%	100%
10.9.3 Información públicamente disponible.	90%	95%	100%	100%
10.10 Supervisión.	**50%**	**90%**	**90%**	**90%**

10.10.1 Registros de auditoría.	50%	90%	90%	90%
10.10.2 Supervisión del uso del sistema.	50%	90%	90%	90%
10.10.3 Protección de la información de los registros.	50%	90%	90%	90%
10.10.4 Registros de administración y operación.	50%	90%	90%	90%
10.10.5 Registro de fallos.	50%	90%	90%	90%
10.10.6 Sincronización del reloj.	50%	90%	90%	90%

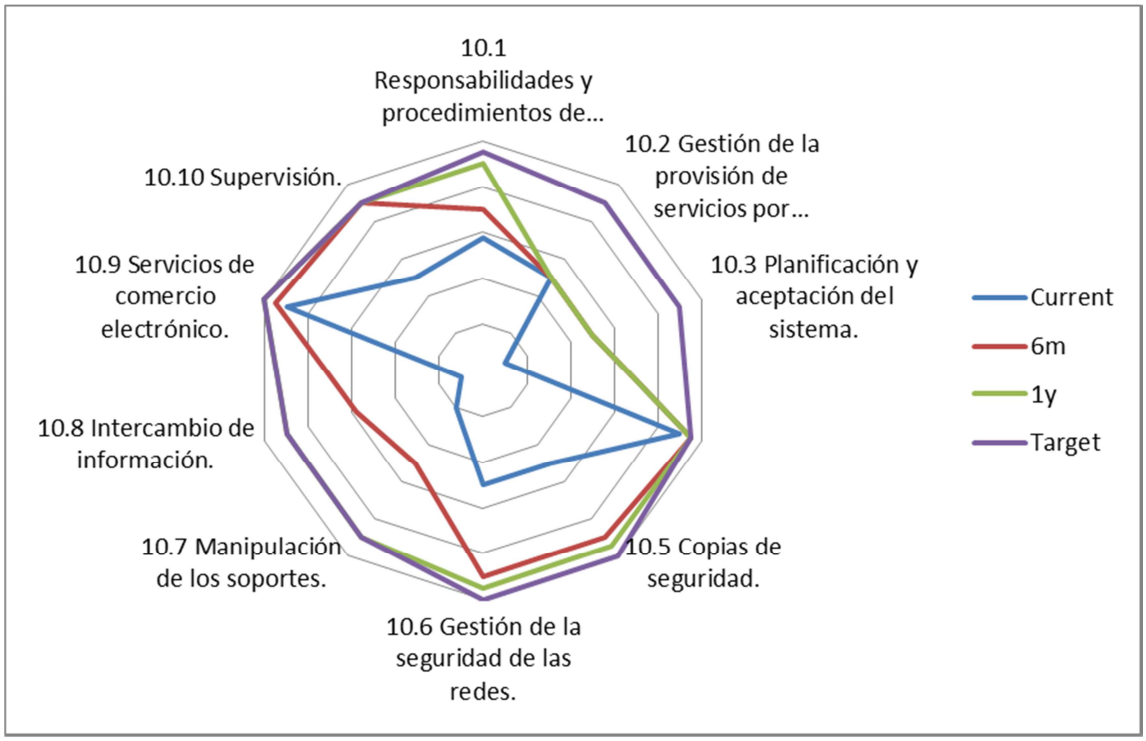
L'empresa ja contempla la segregació de tasques d'una banda[10.1.3] i la separació dels recursos de desenvolupament, prova i producció[10.1.4] d'una banda, però no trobem una documentació pròpia per als processos, si no que són els propis treballadors els que porten a terme aquests processos. D'altra banda, no trobem una documentació d'aquests procediments[10.1.1] ni una gestió pròpiament dita d'aquests canvis[10.1.2].

Per una banda, es pretén millorar la documentació i la gestió durant la segona fase del procés(1 any), i un cop assolida aquesta fita, l'objectiu final seria establir un procés gestionat i mesurable.

Tant els desktops dels usuaris com els portàtils, abans d'entregar-se als propietaris, són dotats amb un programa d'antivirus, que s'actualitza contra el servidor, passant pel servidor de l'empresa, que es qui filtra les actualitzacions[10.4.1][10.4.2]. Aquest procés està definit, però recau en el coneixement de l'equip de sistemes. En aquesta primera fase es vol crear un procés mesurat i gestionable, el qual serà el nostre objectiu final.

Les còpies de seguretat[10.5.1] es realitzen diàriament, de manera programada per l'equip de sistemes. En la primera fase es vol documentar i gestionar aquest procés.

Al tractar-se d'una empresa de venta online, inicialment ja existeixen processos definits per al comerç electrònic[10.0.1], transaccions en línia[10.9.2] i informació públicament disponible[10.9.3], els programadors, juntament amb l'equip de sistemes, són els encarregats de gestionar aquest aspecte. El que es pretén durant la primera fase és crear un procés gestionat, amb l'objectiu final d'optimitzar aquests aspectes de la seguretat per tal d'assegurar una de les parts més importants d'aquest negoci.



11. Control d'accés

CONTROL	Current	6m	1y	Target
11. CONTROL DE ACCESO.	**66%**	**89%**	**91%**	**92%**
11.1 Requisitos de negocio para el control de acceso.	**50%**	**90%**	**90%**	**92%**
11.1.1 Política de control de acceso.	50%	90%	90%	100%
11.2 Gestión de acceso de usuario.				
11.2.1 Registro de usuario.	90%	90%	90%	90%
11.2.2 Gestión de privilegios.	90%	90%	90%	90%
11.2.3 Gestión de contraseñas de usuario.	90%	90%	90%	90%
11.2.4 Revisión de los derechos de acceso de usuario.	50%	90%	90%	90%
11.3 Responsabilidades de usuario.	**50%**	**90%**	**90%**	**90%**
11.3.1 Uso de contraseñas.	50%	90%	90%	90%
11.3.2 Equipo de usuario desatendido.	50%	90%	90%	90%
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	50%	90%	90%	90%
11.4 Control de acceso a la red.	**95%**	**95%**	**95%**	**95%**
11.4.1 Política de uso de los servicios en red.	95%	95%	95%	95%
11.4.2 Autenticación de usuario para conexiones externas.	95%	95%	95%	95%

11.4.3 Identificación de los equipos en las redes.	95%	95%	95%	95%
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.	95%	95%	95%	95%
11.4.5 Segregación de las redes.	95%	95%	95%	95%
11.4.6 Control de la conexión a la red.	95%	95%	95%	95%
11.4.7 Control de encaminamiento (routing) de red.	95%	95%	95%	95%
11.5 Control de acceso al sistema operativo.	**64%**	**95%**	**95%**	**955**
11.5.1 Procedimientos seguros de inicio de sesión.	95%	95%	95%	95%
11.5.2 Identificación y autenticación de usuario.	95%	95%	95%	95%
11.5.3 Sistema de gestión de contraseñas.	95%	95%	95%	95%
11.5.4 Uso de los recursos del sistema.	50%	95%	95%	95%
11.5.5 Desconexión automática de sesión.	50%	95%	95%	95%
11.5.6 Limitación del tiempo de conexión.	0%	95%	95%	95%
11.6 Control de acceso a las aplicaciones y a la información.	**90%**	**90%**	**90%**	**95%**
11.6.1 Restricción del acceso a la información.	90%	90%	90%	95%
11.6.2 Aislamiento de sistemas sensibles.	90%	90%	90%	95%
11.7 Ordenadores portátiles y teletrabajo.	**30%**	**70%**	**90%**	**90%**
11.7.1 Ordenadores portátiles y comunicaciones móviles.	10%	50%	90%	90%
11.7.2 Teletrabajo.	50%	90%	90%	90%

Primerament, cal esmentar que no es troba una política de control d'accés[11.1.1], no obstant , el personal de sistemes són els encarregats de donar els accessos pertinents, un coneixement que roman en el seu departament. En la primera fase es crearà un procés definit, amb l'objectiu final d'optimitzar el procés al màxim.

Existeixen procediments per al registre de d'usuaris [11.2.1], gestió de privilegis[11.2.2] i gestió de contrasenyes[11.2.3], en canvi tot i

que quan algun treballador abandona l'empresa se li revoquen els seus permisos, no es realitza una revisió de drets d'accés[11.2.4] cada cert temps, cosa que pot provocar accessos a informació de personal de la companyia que ja no hauria de tenir. Per a ambdós controls, es vol crear un procés definit durant la primera fase, el qual serà l'objectiu final a mantenir.

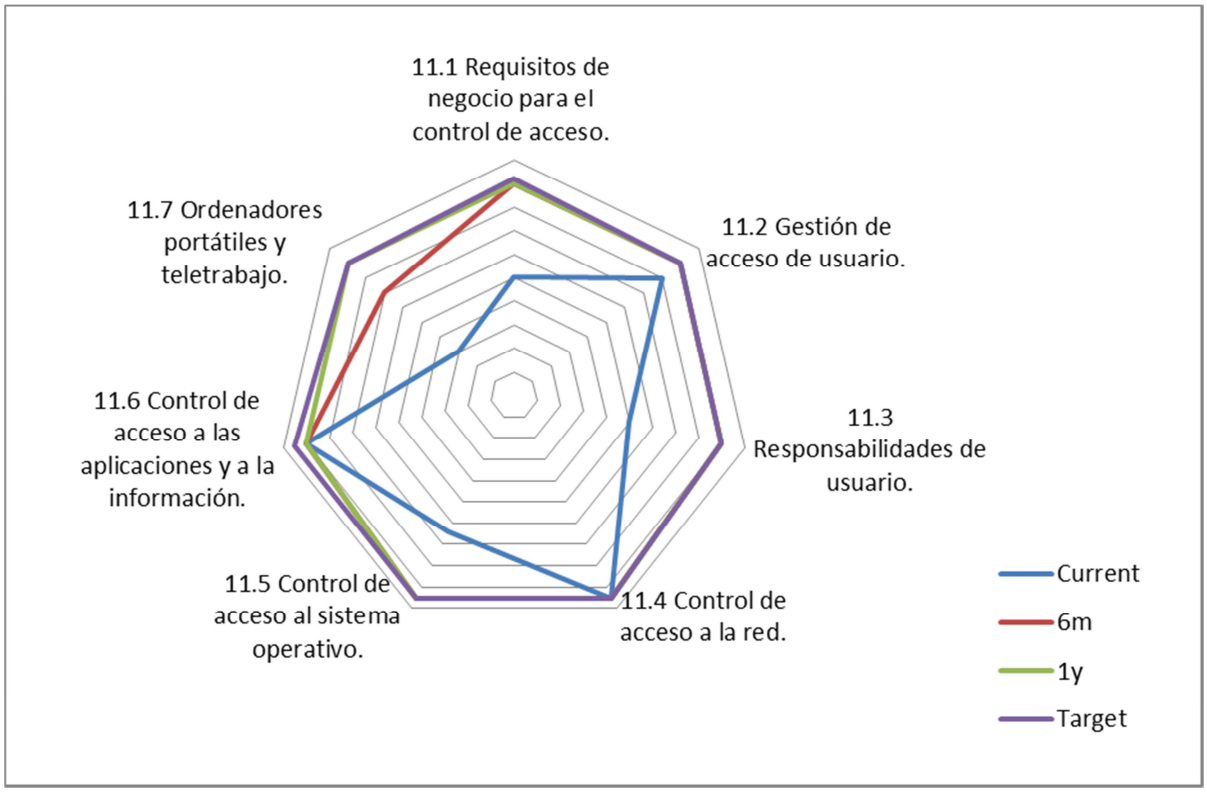
Pel que fa als controls d'accés a la xarxa[11.4], es controlen els accessos a serveis interns i externs connectats a la xarxa ja que existeixen Firewalls entre les diferents xarxes de la organització i la xarxa pública. En aquest aspecte, la organització no requerirà de cap millora.

Pel que fa al control d'accés al sistema operatiu[11.5], actualment es disposa d'un procediment segur per a iniciar sessió,[11.5.1] loguejant-se directament contra el domini de l'empresa mitjançant usuari i contrasenya[11.5.2], unes contrasenyes que han de contenir un nombre, una lletra majúscula, una minúscula i un símbol[11.5.3].

Un cop loguejats, els usuaris són conscients que han de tancar la seva sessió[11.5.5], encara que actualment no ho dictamina cap política, d'altra banda, no existeix cap mecanisme per a limitar el temps de connexió d'un usuari[11.5.6].

Com es comenta anteriorment, tots els treballadors tenen un usuari personal i aquest usuari tindrà o no tindrà accés a certes aplicacions i informació depenent del seu rang[11.6.1][11.6.2].

No trobem cap política per a les activitats de teletreball[11.7.1], no obstant abans de poder realitzar el procés, són comunicades unes mesures bàsiques de seguretat per part de l'equip de sistemes.



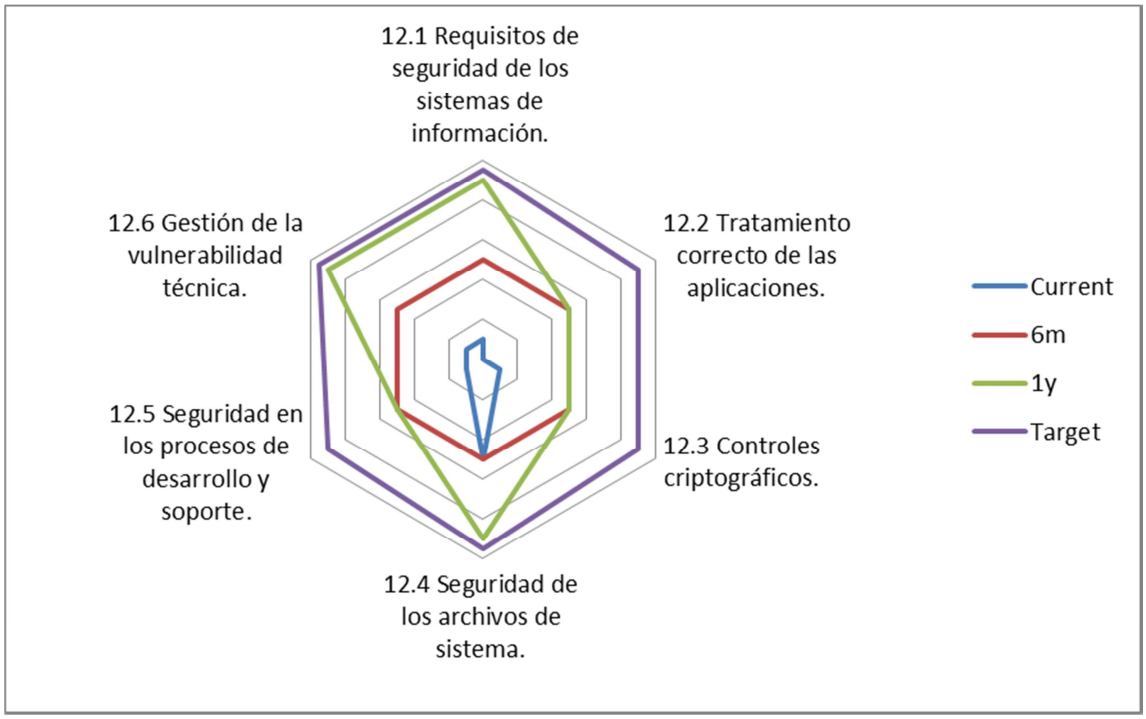
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació.

CONTROL	Current	6m	1y	Target
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	**15%**	**70%**	**90%**	**93%**
12.1 Requisitos de seguridad de los sistemas de información.	**10%**	**50%**	**90%**	**95%**
12.1.1 Análisis y especificación de los requisitos de seguridad.	10%	50%	90%	95%
12.2 Tratamiento correcto de las aplicaciones.	**0%**	**50%**	**50%**	**90%**
12.2.1 Validación de los datos de entrada.	0%	50%	50%	90%
12.2.2 Control del procesamiento interno.	0%	50%	50%	90%
12.2.3 Integridad de los mensajes.	0%	50%	50%	90%
12.2.4 Validación de los datos de salida.	0%	50%	50%	90%
12.3 Controles criptográficos.	**10%**	**50%**	**50%**	**90%**
12.3.1 Política de uso de los controles criptográficos.	10%	50%	50%	90%

12.3.2 Gestión de claves.	10%	50%	50%	90%
12.4 Seguridad de los archivos de sistema.	**50%**	**50%**	**90%**	**95%**
12.4.1 Control del software en explotación.	50%	50%	90%	95%
12.4.2 Protección de los datos de prueba del sistema.	50%	50%	90%	95%
12.4.3 Control de acceso al código fuente de los programas.	50%	50%	90%	95%
12.5 Seguridad en los procesos de desarrollo y soporte.	**10%**	**50%**	**50%**	**90%**
12.5.1 Procedimientos de control de cambios.	10%	50%	50%	90%
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	0%	50%	50%	90%
12.5.3 Restricciones a los cambios en los paquetes de software.	10%	50%	50%	90%
12.5.4 Fugas de información.	10%	50%	90%	90%
12.5.5 Externalización del desarrollo de software.	NA	NA	NA	NA
12.6 Gestión de la vulnerabilidad técnica.	**10%**	**50%**	**90%**	**95%**
12.6.1 Control de las vulnerabilidades técnicas.	10%	50%	90%	95%

Inicialment, la creació de nous sistemes d'informació, com la millora dels existents no especifiquen uns requeriments dels controls de seguretat[12.1.1], això provoca que les mesures de seguretat d'aquest control es divideixin entre un control inicial o inexistent. Menció especial a la subcontractació del desenvolupament software[12.5.5], aquest control no seria aplicable ja que en la mateixa empresa es desenvolupa el software propi a utilitzar.

En aquest control, es pretén definir una política envers la especificació de requeriments de seguretat durant la primera fase, i a partir d'aquí anar conscienciant els treballadors en aquesta fase, per a durant la segona i tercera poder definir processos.



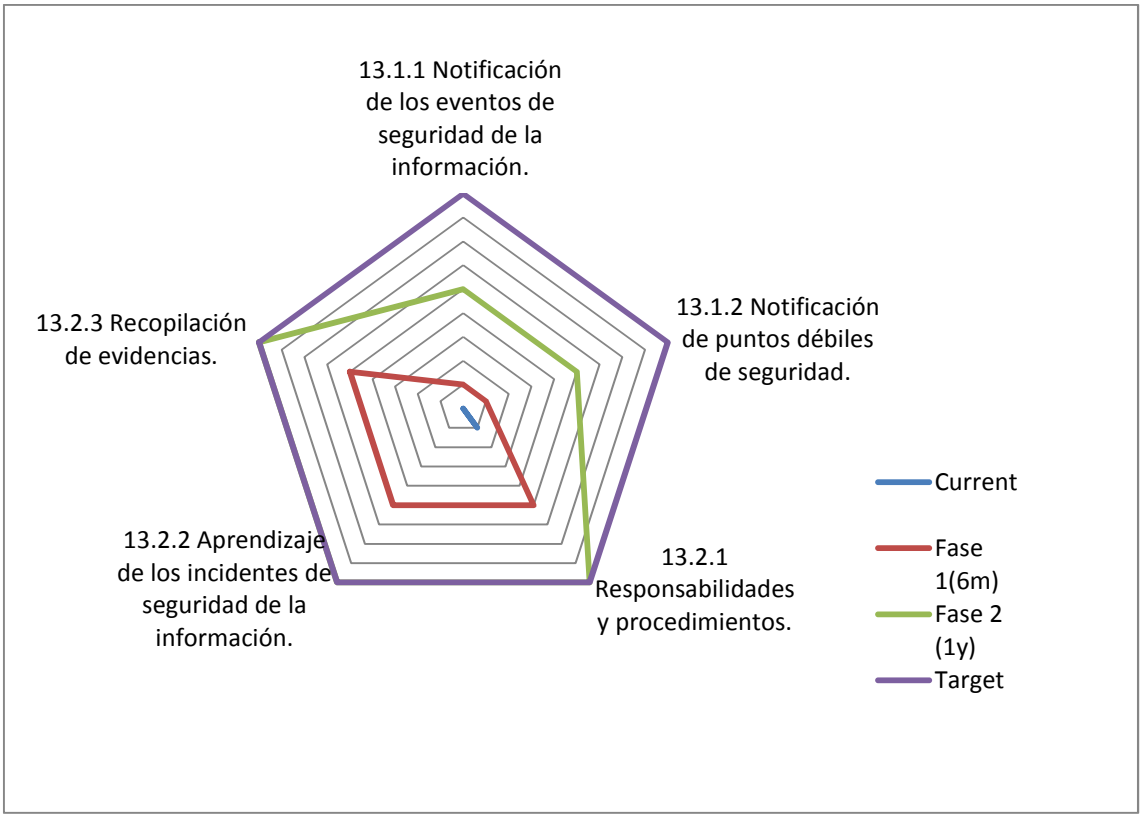
13. Gestió d'incidents en la seguretat de la informació.

CONTROL	Current	6m	1y	Target
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**10%**	**80%**	**90%**	**90%**
13.1 Notificación de eventos y puntos débiles de seguridad de la información.	**10%**	**70%**	**90%**	**90%**
13.1.1 Notificación de los eventos de seguridad de la información.	10%	70%	90%	90%
13.1.2 Notificación de puntos débiles de seguridad.	10%	70%	90%	90%
13.2 Gestión de incidentes y mejoras de seguridad de la información.	**10%**	**90%**	**90%**	**90%**
13.2.1 Responsabilidades y procedimientos.	30%	90%	90%	90%
13.2.2 Aprendizaje de los incidentes de seguridad de la información.	0%	90%	90%	90%
13.2.3 Recopilación de evidencias.	0%	90%	90%	90%

En aquests moments, els empleats no solen notificar esdeveniments de seguretat[13.1.1] o punts dèbils de seguretat[13.1.2], degut al desconeixement i a la falta d'unes pautes a seguir. No obstant, alguns treballadors esporàdicament han notificat alguna incidència, per la qual cosa trobem aquest processos en un estat inicial.

D'altra banda, les responsabilitats[13.2.1] recauen sobre l'informàtic que s'encarrega dels sistemes, que actualment és l'únic que gestiona la seguretat, sense haver-hi un procés definit. No existeixen mecanismes per recopilar o monitoritzar aquest tipus d'incidències.[13.2.2][13.2.3].

En aquest apartat, durant la primer fase es vol conscienciar als treballadors per a que notifiquin aquests esdeveniments, alhora que es volen crear processos definits per a la gestió d'incidents. Durant la segona fase, es vol assolir la creació d'un procés i donar-lo a conèixer per a que es pugin notificar aquestes incidències.

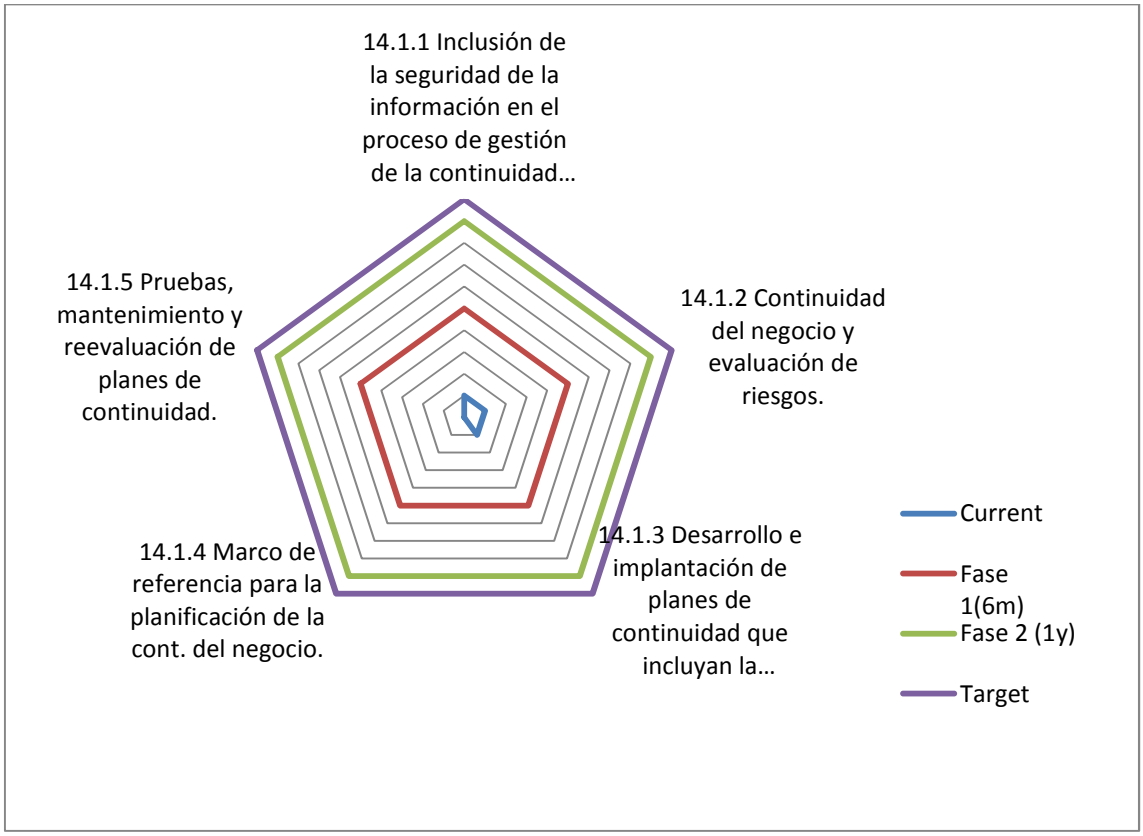


14. Gestió de la continuïtat del negoci.

CONTROL	Current	6m	1y	Target
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**6%**	**50%**	**90%**	**100%**
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	**6%**	**50%**	**90%**	**100%**
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	10%	50%	90%	100%

14.1.2 Continuidad del negocio y evaluación de riesgos.	10%	50%	90%	100%
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	10%	50%	90%	100%
14.1.4 Marco de referencia para la planificación de la cont. del negocio.	0%	50%	90%	100%
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.	0%	50%	90%	100%

En aquest control, en general no trobem implantat un procés de continuïtat del negoci per a reduir la interrupció causada per desastres i falles de seguretat.
La seguretat de la informació està inclosa en el procés de continuïtat del negoci[14.1.1] de manera molt lleu, en potenciar això, només hi treballa una persona i no hi dedica gaire temps. Arrel d'això, durant la primera fase del procés, es vol aconseguir definir un procés involucrant a més persones per tal de tenir una resposta en cas de que sorgís algun dels esmentats problemes.
Durant la següent fase, es vol assolir un model gestionat i mesurable, i per últim durant la última fase es vol arribar a assolir un model optimitzat



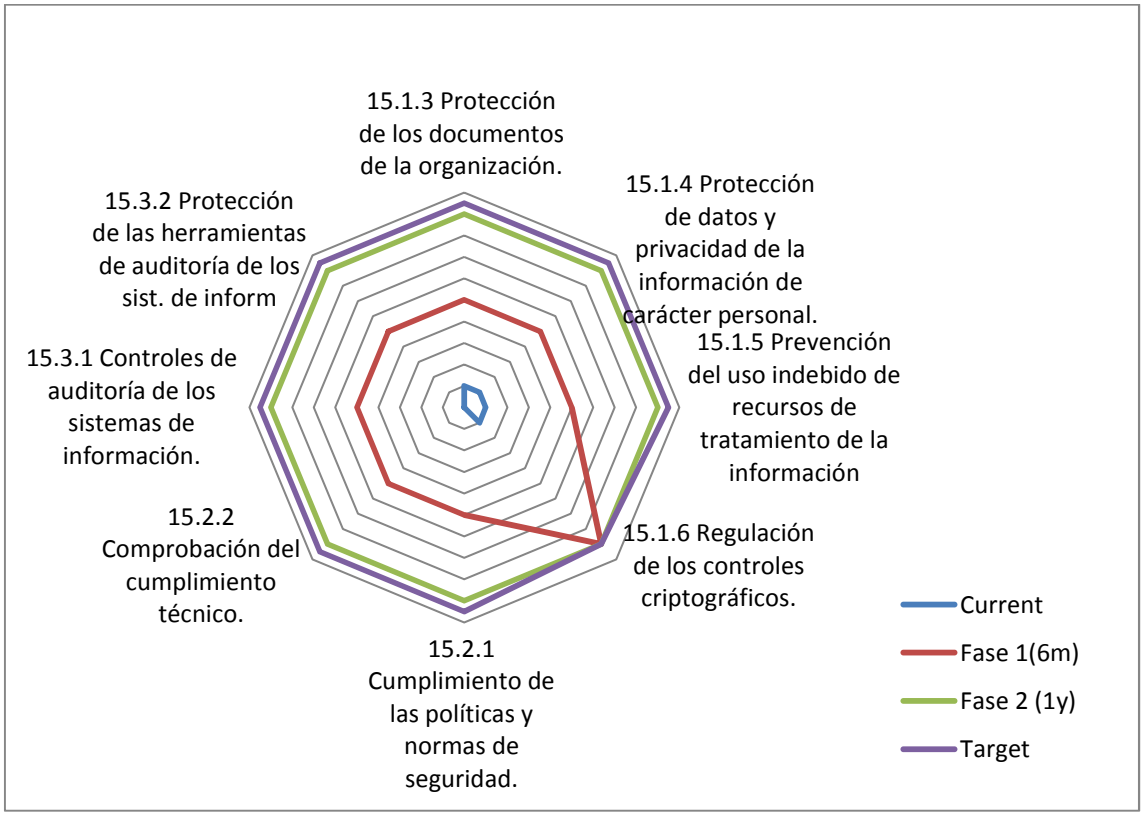
15. Compliment.

CONTROL	Current	6m	1y	Target
15. CUMPLIMIENTO.	**3%**	**53%**	**90%**	**95%**
15.1 Cumplimiento de los requisitos legales.	**10%**	**60%**	**90%**	**91%**
15.1.1 Identificación de la legislación aplicable.	NA	NA	NA	NA
15.1.2 Derechos de propiedad intelectual (DPI).	NA	NA	NA	NA
15.1.3 Protección de los documentos de la organización.	10%	50%	90%	95%
15.1.4 Protección de datos y privacidad de la información de carácter personal.	10%	50%	90%	95%
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información	10%	50%	90%	95%
15.1.6 Regulación de los controles criptográficos.	10%	90%	90%	90%
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	**0%**	**50%**	**90%**	**95%**
15.2.1 Cumplimiento de las políticas y normas de seguridad.	0%	50%	90%	95%
15.2.2 Comprobación del cumplimiento técnico.	0%	50%	90%	95%
15.3 Consideraciones sobre las auditorías de los sistem. de información.	**0%**	**50%**	**90%**	**95%**
15.3.1 Controles de auditoría de los sistemas de información.	0%	50%	90%	95%
15.3.2 Protección de las herramientas de auditoría de los sist. de inform	0%	50%	90%	95%

Tot i que el departament de RRHH s'encarrega de la revisió de les clàusules a nivell estatal, els encarregats de definir, documentar i regular els requisits estatutaris[15.1.1] no es troben en l'abast d'aquest SGSI, degut a que es realitzen des de fora de la seu en qüestió. El mateix succeeix amb els drets de propietat intel·lectual[5.1.2], ja que aquest aspecte es gestiona des de la seu central.

D'altra banda, les dades emmagatzemades en la pròpia seu, no tenen un procediment estipulat i definit. Estan basats en el coneixement i la bona fe del departament corresponent. D'aquesta manera, els controls [5.1.3] [5.1.4] [5.1.5] [5.1.6] que afecten a la informació sensible tindran un nivell de de compliment L1. En aquests apartats es pretén millorar durant la primera fase definint un procés(L3) i arribar a L4 durant la segona fase.

Pel que fa al compliment de les polítiques[15.2], actualment no es realitzen revisions regulars de la seguretat dels sistemes de la informació, ni es revisa regularment els sistemes de seguretat[15.3], degut a la inexistència de les polítiques. En ambdós processos es pretén definir un procés(L3) durant la primera fase i aconseguir arribar a L4 durant la segona fase.

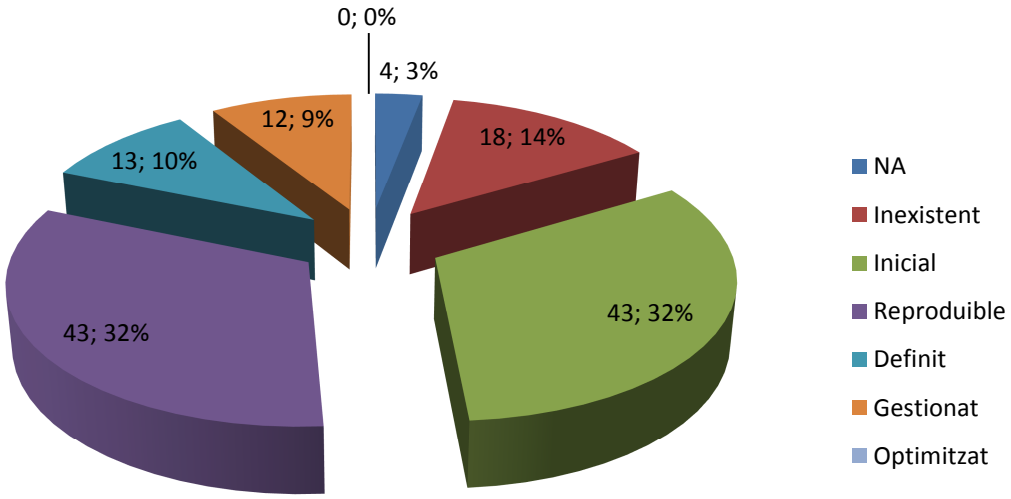


Resultats Finals

En aquests gràfic podem observar el percentatge de compliment dels controls en cadascuna de les fases.

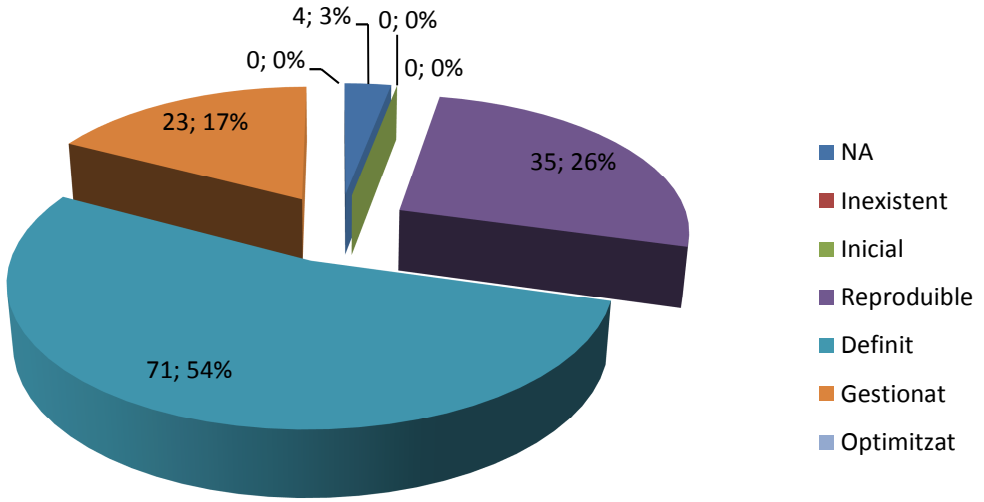
Current

Estat actual del sistema.



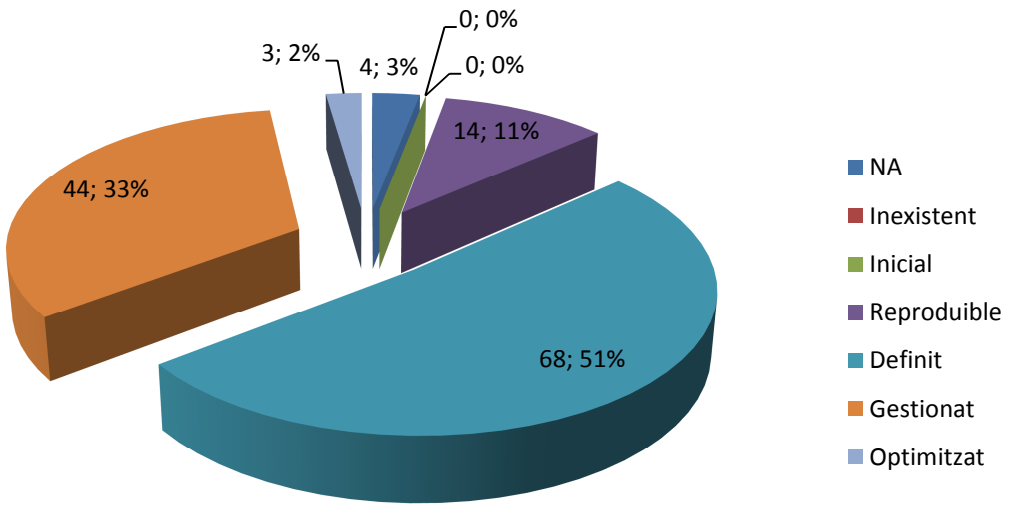
Primera Fase(6m)

Nivell de compliment transcorreguts sis mesos.



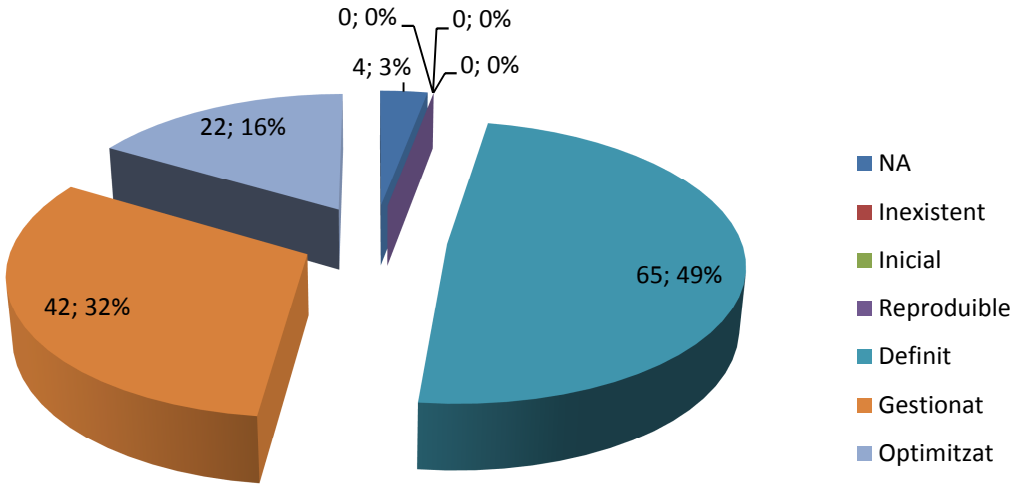
Segona Fase(1y)

Nivell de compliment transcorregut un any.



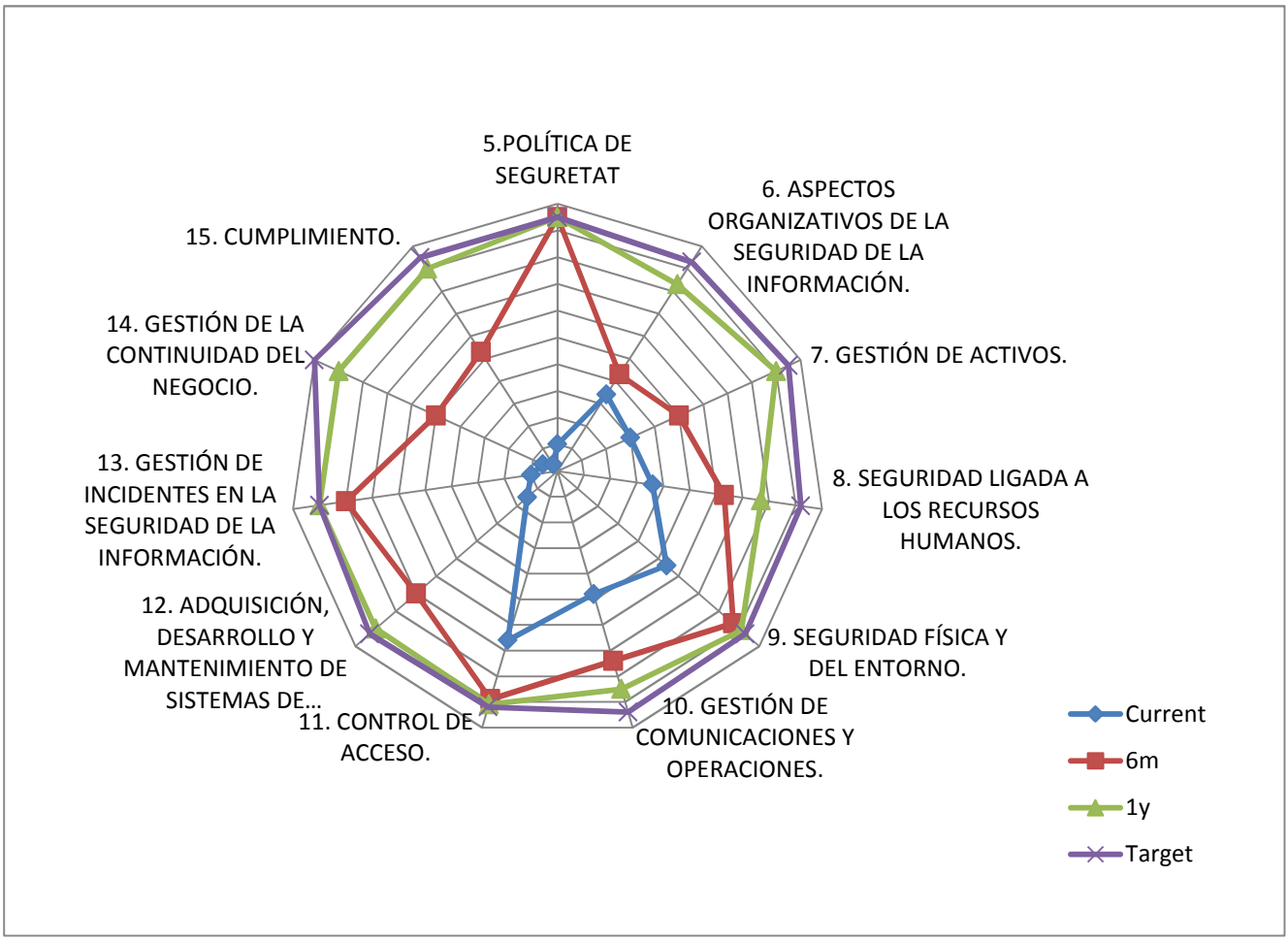
Target

Nivell de compliment final



Gràfica radial dels controls ISO.

En aquesta gràfica observem el nivell de compliment per cadascun dels controls ISO, el seu estat inicial i durant les tres fases del procés.



Annex 3 – Proposta de Projectes

Projecte 1- Creació d'una Política de Seguretat

Objectiu

L'objectiu final, a tres anys vista d'aquest projecte serà la realització d'una política estructurada i constantment en revisió adaptant-la a les necessitats de l'empresa.

Descripció

Es crea una política de seguretat adient a les necessitats de la companyia.

L'abast del Pla Director de Seguretat engloba els serveis més crítics oferts des de les oficines centrals de XXXX S.L.

S'inclouen dins de l'abast del SGSI a tot el personal, sistemes informàtics i actius que la organització utilitza per a la presentació d'aquests serveis, d'acord a la definició que en cada moment estigui vigent en els mateixos.

La prestació dels serveis definits anteriorment es realitza des de la ubicació física: C/ Guillem Gimeno nº 22 plantes 3ª i 4ª, Barcelona

Per últim, quedaran excloses de l'abast les diferents seus de la organització en els altres països.

Beneficis

Aquesta política s'aplicarà a curt termini amb la finalitat de realitzar les millores pertinents en la organització seguint uns criteris que vindran marcats per la mateixa.

Cost

RECURS	DESCRIPCIÓ	QUANTITAT	COST TOTAL
Altres	Documentació ISO 27001:2005	1	36,64 €
Altres	Documentació ISO 27002:2009	1	72 €
TOTAL			108,34€

A aquest cost s'haurà d'afegir la part proporcional dels sous de les persones de la organització que s'encarreguen de la realització de la política.

Motivació

Millora dels controls ISO27002:2005, 5.1.1 i 5.1.2

Projecte 2 - Assignació d'Actius

Objectiu

Durant la primera fase, l'objectiu simplement serà la captació d'informació sobre els actius i la assignació provisional de diferents actius als treballadors.

L'objectiu durant la segona fase serà que tots els actius deuran ser justificats i tenir-hi assignat un propietari. Al propietari de l'actiu se li assignarà la responsabilitat de manteniment dels controls adients.

Aquest procés tindrà com a objectiu final tenir un inventari d'actius gestionat i mesurable.

Descripció

Amb aquesta informació, el departament de sistemes elaborarà una base de dades mitjançant Microsoft Access amb les taules corresponents als criteris anteriors.

Beneficis

Poder consultar qualsevol actiu mitjançant consultes a la base de dades de Microsoft Access i evitar la no devolució o la utilització per part de persones no autoritzades de determinats actius.

Cost

El cost de la millora ve determinat per la part proporcional del sou de les persones encarregades del seu desenvolupament.

Motivació

Millora dels controls ISO27002:2005 en els punts 8.3.1, 8.3.2 i 8.3.2 i també el 7.1.1 i 7.1.2.

Projecte 3- Emmagatzematge de Backups en ubicació remota.

Objectiu

Durant la primera fase ja es pretén contractar el servei d'allotjament.

En la segona fase es pretén donar a conèixer la mesura i documentar-la, fins arribar a un objectiu final mesurable.

Descripció

Emmagatzemar e una ubicació remota les copies recents de la informació, juntament amb els procediments documentats de restauració; es guardaran a una distància suficient com per a evitar danys provinents d'un desastre en la zona principal.

Beneficis

Evitar la pèrdua de les còpies de seguretat degut a la materialització d'una amenaça de tipus ambiental en l'edifici de l'empresa.

Cost

El cost ve determinat de llogar una ubicació per a depositar les copies(70 €/ mes).

Motivació

Millora del control ISO27002:2005, 10.5.1

Projecte 4 - Creació de normativa de passwords.

Objectiu

Durant la primera fase es crea una norma sobre l'ús de les contrasenyes. En la segona fase serà difosa als treballadors de la organització mitjançant el correu electrònic. Finalment, l'objectiu es obtenir un control gestionat sobre les contrasenyes.

Descripció

Creació d'una política que deurà seguir el personal de l'empresa sobre les contrasenyes per accedir a aplicacions i correus electrònic.

Beneficis

Evitar les contrasenyes genèriques o fàcils d'endevinar, evitant així els accessos no desitjats que puguin afectar la disponibilitat dels processos o la integritat de la informació.

Cost

El cost de la millora ve determinat per la part proporcional del sou de les persones encarregades del seu desenvolupament.

Motivació

Millora del control ISO27002:2005, 11.3.1

Projecte 5 - Millora de l'accés físic a oficines.

Objectiu

Durant la segona fase es faran reformes per adaptar les dues plantes a la nova manera d'accés.

Descripció

S'implantarà a un control d'accés a les dues plantes de la empresa mitjançant les targetes utilitzades per entrar a l'edifici. a través de les altes dues empreses que cohabiten a l'edifici pugin accedir a les dependències de la organització.

Beneficis

Evitarem la possibilitat que personal no autoritzat entri a les oficines.

Cost

RECURS	DESCRIPCIÓ	QUANTITAT	COST TOTAL
Personal	Reforma per accedir a oficines	2	1000€

Motivació

Millora dels controls ISO27002:2005 , 9.1.2 I 9.1.3

Projecte 6 - Protecció d'accés al CPD.

Objectiu

L'objectiu durant la primera fase serà la compra i instal·lació del dispositiu. Durant la segona fase del projecte es crearan les normes i polítiques que es seguiran per decidir la política d'accessos al CPD. La tercera fase te com a objectiu obtenir un control regulat i documentat amb polítiques definides per a l'accés.

Descripció

Es canviarà l'actual sistema d'entrada amb clau per un sistema d'entrada mitjançant la mateixa targeta d'accés a la organització, que haurà de ser

proveïda dels permisos adients i que s'haurà de validar a la porta, juntament amb la introducció d'un codi personal i intransferible.

Els codis s'hauran de canviar cada trimestre i a les reunions del Comitè de Seguretat es validaran les persones autoritzades per a l'accés al CPD.

Beneficis

Amb la implantació d'aquesta mesura s'obtindrà una major seguretat en una àrea restringida, protegint-la així de possibles atacs intencionats com no intencionats. Es millorarà la integritat, confidencialitat i disponibilitat.

Cost

RECURS	DESCRIPCIÓ	QUANTITAT	COST TOTAL
Hardware	Lector amb teclat per control d'accés PROXPRO® - DS018	1	300 €
Personal	Instal·lació i configuració	1	150 €
TOTAL			450 €

Motivació

Millora dels controls 9.1.2 i 9.1.5 de la norma ISO 27002:2005