Elaboració d'un plà de Seguretat de la Informació

Gimeno Domènech, Guillem

Introducció

- La informació és un valuós actiu del que depèn el bon funcionament d'una organització.
- Mantenir la seva integritat, confidencialitat i disponibilitat és essencial per a assolir els objectius de negoci.
- La implantació d'un SGSI és una eina o metodologia que qualsevol empresa pot utilitzar, i que a més a més oferirà una sèrie de garanties envers altres empreses.

Projecte

- Què és un SGSI?
  - Un Sistema de Gestió de la Informació és una forma d'entendre, de dissenyar i de regular els processos de negoci de l'empresa des d'una perspectiva molt més eficient.
  - Amb aquesta metodologia de treball es redueix el risc de qualsevol tipus de manipulació de la informació que pugui traduir-se en robatori, pèrdua o manipulació.

Avantatges

- La implantació d'un SGSI en la organització generarà 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.

Estàndards de Gestió de Seguretat de la Informació

- ISO / IEC 27001
  - Establir
  - Implementar
  - Operar
  - Supervisar
  - Revisar
  - Mantenir
  - Millorar
- ISO / IEC 27002:2005
  - Guia de bones pràctiques.
  - 11 Dominis
  - 39 Objectius de control
  - 133 Controls

Metodologia

- Pla director de Seguretat, model PDCA
  - Analitzar i detallar el nostre inventari d'actius.
  - Estudiar les amenaces a què estan exposats.
  - Estudiar l'impacte potencial d'aquestes amenaces.
  - Proposar un pla d'acció per lluitar contra aquestes amenaces.
  - Avaluar l'impacte residual un cop aplicat el pla d'acció

Fases del projecte

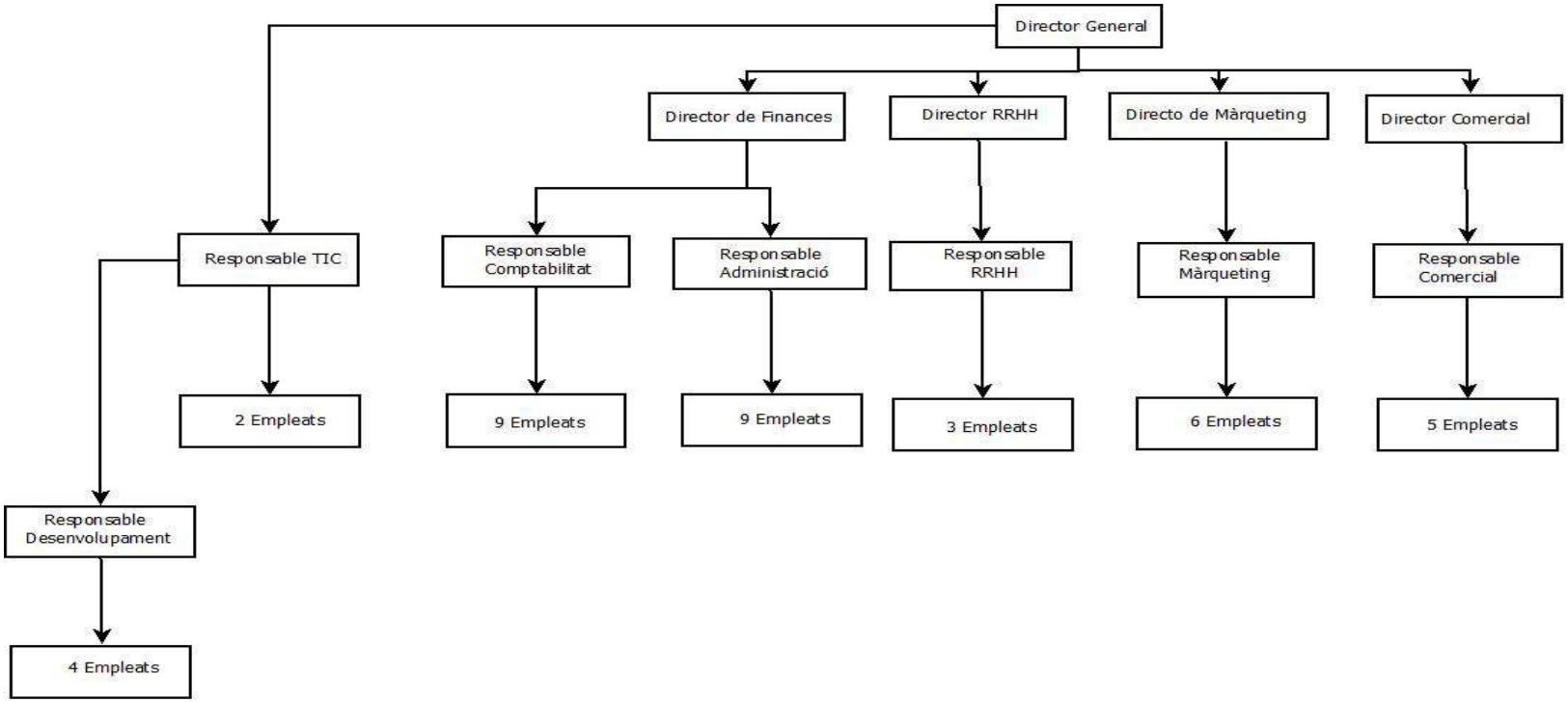
- Fase 1: Contextualització i documentació
- Fase 2: Objectius del Pla Director
- Fase 3: Estat del Risc: Identificació i valoració dels Actius i Amenaces
- Fase 4: Auditoria i compliment de la ISO:IEC 27002:2005
- Fase 5: Projectes de millora
- Fase 6: Presentació de resultats i conclusions.

Fase 1: Contextualització i documentació

- L'empresa XXXXX es una organització exclusivament dedicada a la venta de productes tèxtils online.
- L'abast del projecte estarà centrat en la seu de Barcelona.
- L'empresa té en nòmina 50 empleats
- No existeix cap SGSI prèviament implantat.

Fase 1: Contextualització i documentació

Estructura organitzativa:



Fase 2: Objectius del Pla Director

- Es defineixen estratègies i polítiques cooperatives TIC.

- Implicació de la direcció.
  - S'ha creat el Comitè de Seguretat: Encarregat d'assignar rols i funcions en matèria de seguretat
  - S'ha nomenat un Responsable de Seguretat de la Informació: El rol recau en el responsable TIC.
  - S'ha inclòs la Seguretat de la Informació en l'ordre del dia de les reunions.

Fase 2: Objectius del Pla Director

Estructura del Comitè de Seguretat:

<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>

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

- Actius: Elements que es deuen protegir envers riscos i amenaces per a assegurar un correcte funcionament del negoci.

- Dependències: 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.

- Amenaces (MAGERIT)
  - Desastres naturals
  - D’origen industrial
  - Error i fallades no intencionades
  - Atacs intencionats

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

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

- Identificació d'Actius Essencials.
  - 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.

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

[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

[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

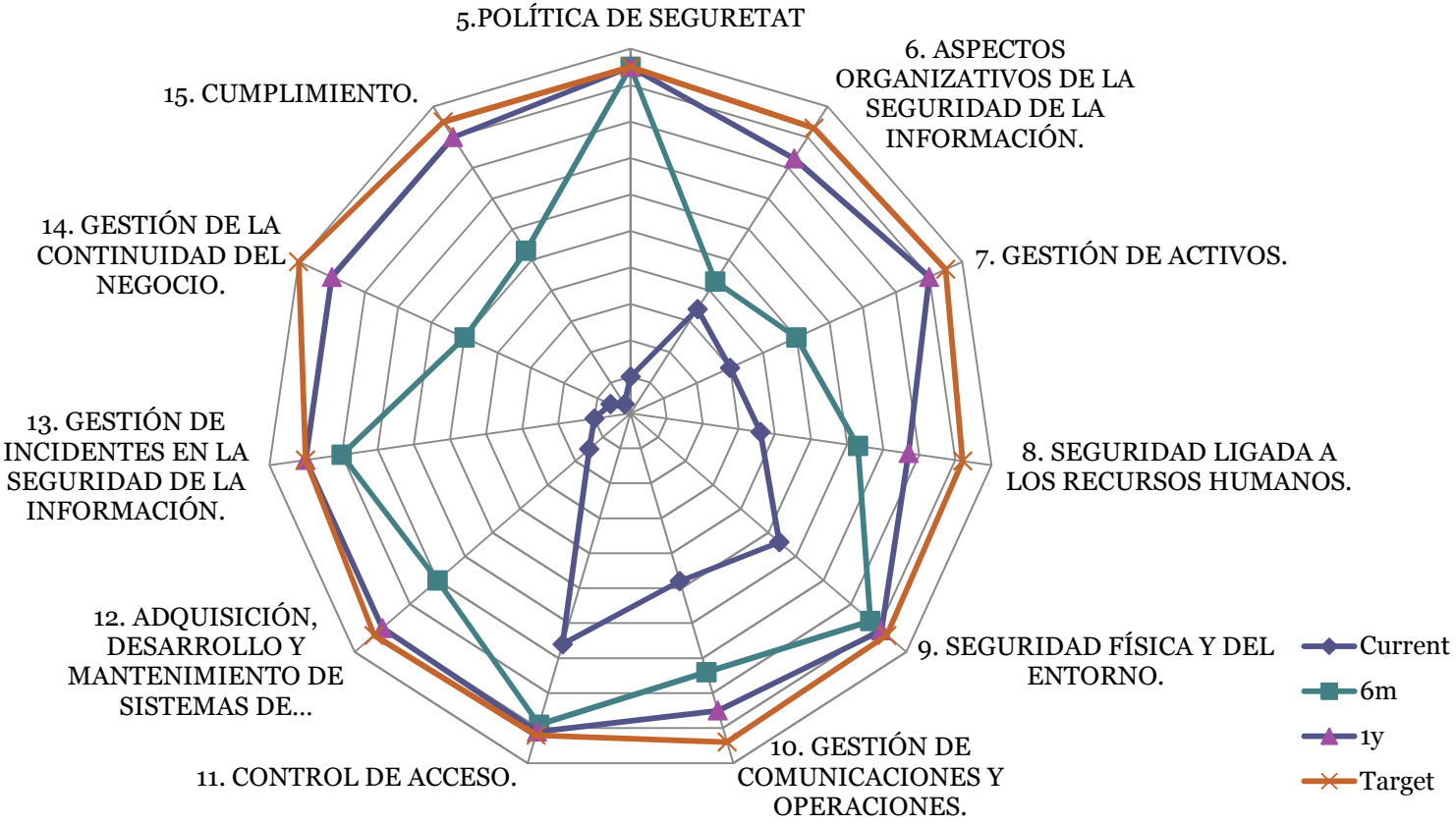
[Actiu]Estacions de treball
- Oficines

[Actiu]Xaxa LAN
- Servidors Xarxa Interna.

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

- L'estàndard ISO 27002:2005 consta de 133 controls de seguretat repartits en 11 dominis de seguretat.
- Anàlisi de la maduresa dels 133 control de l'estàndard ISO 27002:2005 basat en el Model de Maduresa de la Capacitat (CMM).
- Anàlisi de compliment en les quatre fases definides.
  - 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.

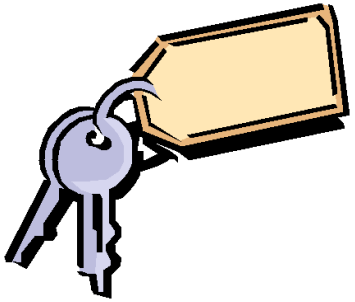
Fase 4: Auditoria i compliment de la ISO:IEC 27002:2005



Fase 5: Projectes de millora

- Un cop conegut l'estat de la seguretat, es plantegen els següents projectes.
  - Creació de la política de Seguretat.
  - Assignació d'actius
  - Emmagatzematge de Backups en ubicació remota.
  - Creació de normativa de Passwords.
  - Millora de l'accés físic a les oficines.
  - Protecció d'accés al CPD.

Fase 5: Projectes de millora(Exemple) Accés al CPD:



- **Descripció**
  - Current: Accés amb clau (50% CCM)
  - Target: Accés amb targeta amb codi personal, amb revisió constant de permisos.(95% CCM)
- **Beneficis**
  - Integritat
  - Confidencialitat
  - Disponibilitat
- **Cost**
  - Lector amb teclat per control d'accés PROXPRO® - DS018
  - = 300€
  - Instal·lació i configuració = 150 €
- **Motivació**
  - Control 9.1.2 i 9.1.5 de la norma ISO 27002:2005

Fase 6: Presentació de resultats i conclusions.

- Un cop posat en funcionament el pla de seguretat, es revisarà periòdicament de manera que es detectin possible desviacions.
  - Conformitat amb els requisits de l'ISO 27001
  - Conformitats amb la legislació aplicable
  - Conformitat amb els requisits de seguretat identificats
  - Implementats i mantinguts de manera activa
  - Donen el resultat esperat.

Fase 6: Presentació de resultats i conclusions.

- 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.

- El Sistema de Gestió de Seguretat de la Informació s'ha definit en base als riscos a la que està exposada la organització i els aspectes intrínsecs del seu funcionament.

GRÀCIES PER LA VOSTRA ATENCIÓ