efimatica

Pla Director de Seguretat

Consultoria
Seguretat
de la Informació

DESCRIPCIÓ DEL SERVEI

Passeig Gral Mendoza, 1 5è
17001 Girona
972 411 600
cserra@efimatica.com

Cada cop més, les empreses tenen una dependència més alta de la tecnologia per gestionar els processos clau de negoci. Per altra banda, els ciberatacs i altres riscos creixen dia a dia.

Per això, cal disposar d'un pla que permeti tenir una guia per implantar de manera coordinada i continuada mesures de seguretat i procediments per gestionar els riscos identificats que puguin afectar els actius, la seguretat de la informació i el negoci.

Conèixer quins són els riscos que afecten els actius crítics, permet fer-los front posant en marxa les mesures necessàries per garantir la seguretat de la informació.

¿Qué és un Pla Director de Seguretat?

Consisteix en la definició i la priorització d'un conjunt de projectes en matèria de seguretat de la informació amb l'objectiu de reduir els riscos als quals està exposada l'organització fins a uns nivells acceptables, a partir d'una anàlisi de la situació inicial.

Aquesta anàlisi es fa considerant aspectes tècnics, organitzatius, reguladors i normatius, entre d'altres.

Delimitar i establir l'abast

Aquest abast determinarà la magnitud dels treballs i també quin serà el focus principal de la millora després de l'aplicació del pla: un únic departament, per exemple, el de TIC; un conjunt de processos crítics, o uns sistemes específics.

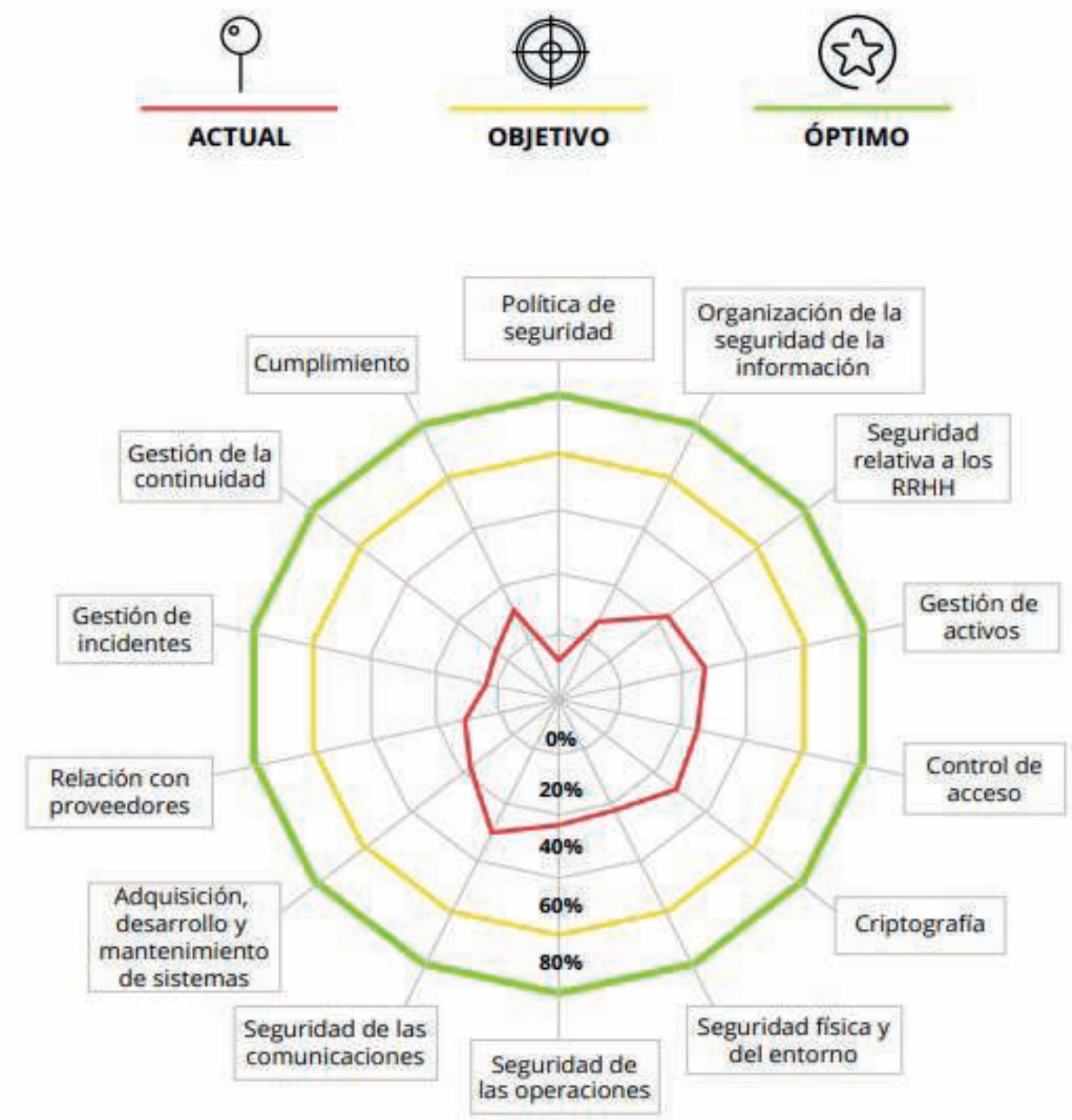
El recomanable és determinar els actius i els processos de negoci crítics, aquells sense els quals l'empresa no pot subsistir.

Fases del projecte

El pla director de seguretat inclou les tasques següents:

1. Analitzar la situació actual de la seguretat de la informació de l'empresa.

Aquesta fase és el punt de partida i inclou les entrevistes al personal clau de l'àrea d'informàtica per conèixer les mesures tècniques, organitzatives i legals implantades. A partir d'aquí obtenim el mapa amb la situació real de la seguretat de la informació, la situació objectiu i l'escenari òptim.



2. Avaluació actual de les situacions de risc de la companyia.

En aquesta fase s'identifiquen els actius, els processos de negoci crítics i les persones amb responsabilitat sobre aquests actius.

S'identifiquen les amenaces i la probabilitat que es materialitzin i afectin els actius.

Els sistemes d'informació estan sotmesos constantment a amenaces, que poden assolir des de fallades tècniques i accidents fins a accions intencionades, més o menys lucratives, de curiositat, espionatge, sabotatge, vandalisme, xantatge o frau.

L'anàlisi del risc estudia aquestes amenaces des del punt de vista de la probabilitat que succeeixin i de quin seria el seu impacte.

a) Identificació i valoració dels actius

Durant aquesta tasca s'identifiquen els actius necessaris perquè el sistema informàtic funcioni i es classifiquen per categoria.

b) Diagnòstic de vulnerabilitats

S'identifiquen les amenaces presents sobre els actius i se n'assignen els impactes.

S'avalua el mal que produeix cada amenaça en cas que es materialitzi una vulnerabilitat sobre un actiu. Es mesura en termes de disminució del nivell de seguretat o del valor de l'actiu.

c) Estudi dels riscos

Es defineixen els mecanismes de seguretat més adequats a les necessitats de l'organització des del punt de vista de la capacitat tecnològica i dels procediments organitzatius necessaris.

S'analitza el risc als actius en funció de la probabilitat i de l'impacte. Es determina el risc intrínsec, calculat sense implantar mesures de seguretat i risc residual, aquell que l'organització està disposada a assumir.

3. Decidir el tratament dels riscos identificats

Arriba el moment de concretar quin és el nivell de risc acceptable per l'empresa i de seleccionar el tractament de cada risc identificat.

La gestió del risc consisteix a assumir, transferir o evitar i eliminar els riscos coneguts mitjançant un pla de seguretat.

L'objectiu és reduir els nivells dels riscs no acceptables.

4. Planificar els projectes

En aquesta fase es detallen les mesures tècniques, organitzatives i legals i també els recursos necessaris per implantar per reduir els riscos identificats.
Les mesures han d'incloure el cost econòmic, els recursos necessaris i les dates d'execució previstes per implantar les accions proposades a curt, mitjà i llarg termini.
Les accions aniran acompanyades de la justificació i la priorització, segons el nivell de risc.

5. Finalització: Presentació i Aprovació del Pla Director de Seguretat

En aquesta fase es fa el tancament formal del projecte, mitjançant l'elaboració i l'aprovació d'un document executiu per al vistiplau de la direcció.
La direcció té la responsabilitat de revisar i aprovar el Pla Director de Seguretat i aportar els recursos necessaris per desplegar els projectes.

Com Efimatica us pot ajudar?

Comptem amb professionals amb dècades d'experiència al sector TIC i al Govern, Risc i Compliment, Protecció de Dades, Auditoria i Consultoria de la Seguretat de la Informació.

El nostre objectiu sempre és aportar a l'empresa la solució més convenient en funció d'exigències i necessitats de cada projecte, tractant cada cas de manera diferent i, per tant, única.

· Adaptació: Ens encarreguem de tot el procés perquè la teva empresa compleixi la llei.

· Suport: Si ja esteu realitzat l'adaptació, us ajudem a resoldre dubtes o dur a terme les tasques o funcions pròpies del DPO.

· Auditoria: Si no estàs segur que la teva companyia compleix la normativa, fem una auditoria per verificar-ho.