MÀSTER INTERUNIVERSITARI DE SEGURETAT DE LES TECNOLOGIES DE LA INFORMACIÓ I DE LA COMUNICACIÓ

PLA DIRECTOR DE SEGURETAT

AJUNTAMENT DE RIBEROLA

RESUM EXECUTIU

TREBALL DE FI DE MÀSTER

Juny 2013

DIRECTOR: Carles Garrigues

CONSULTOR: Arsenio Tortajada

ALUMNE: Ricard Salvat

UOC Universitat Oberta de Catalunya www.uoc.edu

UAB Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

UIB Universitat de les Illes Balears

ÍNDEX

1. MOTIVACIÓ DEL PROJECTE

Actualment, moltes organitzacions i empreses consideren la informació com un dels seus valors més importants. Això és així perquè la disponibilitat, integritat, confidencialitat i autenticitat d'aquesta informació, juntament amb els processos i elements que la tracten, són vitals i indispensables pel funcionament i supervivència d'aquestes empreses i organitzacions.

Les administracions públiques, de la mateixa manera que les empreses i organitzacions, depenen cada cop més de les tecnologies de la informació i la comunicació per realitzar les seves funcions, ja siguin relacionades amb els serveis a la ciutadania o amb altres administracions, entitats o empreses.

Mitjançant l'execució d'aquest projecte, l'Ajuntament de Riberola desitja implantar un **Pla de Seguretat** per tal d'assolir principalment els tres següents objectius:

- Obtenir una visió de l'estat actual de la seguretat en les Tecnologies de la Informació i la Comunicació.
- Proporcionar mesures o actuacions a realitzar a curt o llarg termini per tal de millorar els aspectes crítics que es detectin, seguint uns objectius concrets i definits.
- Assentar les bases per la creació d'un Sistema de Gestió de Seguretat de la Informació (SGSI), per tal de controlar l'evolució de la seguretat de l'organització al llarg del temps.

Addicionalment, al tractar-se d'una administració pública, és requereix el compliment, entre altres, de l'Esquema Nacional de Seguretat (ENS), el qual pràcticament obliga a disposar d'un Sistema de Gestió de Seguretat de la Informació.

Existeixen certes metodologies o normes per tal d'assegurar que les organitzacions tenen en consideració l'estat actual i l'evolució de la seguretat de la informació, així com dels elements tecnològics o físics amb els que interactua. L'actual projecte consisteix en la creació d'un **Pla Director de Seguretat** utilitzant com a marc estàndard de referència la norma **ISO/IEC 27001** (provinent de la ISO 17799) i la **ISO/IEC 27002**, on es tracten requisits i codis de bones pràctiques en la gestió de la seguretat de la informació (“*Information technoloy - Security techniques - Code of pratice for information security management*”). Aquestes bones pràctiques són aptes per qualsevol tipus d'empresa o organització.

L'adaptació d'aquests estàndards facilitarà l'adaptació de l'organització a l'**Esquema Nacional de Seguretat**.

2. ENFOCAMENT DEL PROJECTE

La realització d'aquest projecte s'ha dividit en sis fases:

- Objectius del Pla director de seguretat i anàlisi diferencial respecte ISO/IEC 27001.
- Esquema documental ISO/IEC 27001.
- Anàlisi de riscos.
- Proposta de projectes
- Auditoria del compliment
- Presentació dels resultats

En una primera fase, s'han definit els principals objectius del Pla director de Seguretat, se n'ha determinat l'abast i s'ha realitzat un anàlisi diferencial on es valora la situació actual dels diferents punts de la ISO/IEC 27001 en l'Ajuntament de Riberola. Per tant, s'analitzaran les diferents mesures i procediments de seguretat, així com normatives existents en relació a la Seguretat de la Informació.

En la següent fase, s'han desenvolupat i generat els documents bàsics i algunes plantilles necessàries per l'adaptació a la norma ISO/IEC 27001. Per exemple la Política de seguretat i la gestió i assignació dels diferents rols i responsabilitats dins l'organització en la gestió de la seguretat. També es definirà en aquest punt la metodologia que s'emprarà per realitzar l'anàlisi de riscos en la següent fase.

L'anàlisi de riscos dut a terme en la tercera fase ens aporta:

- Un anàlisi detallat dels actius més essencials relacionats amb la Seguretat de la Informació.
- Un estudi de les possibles amenaces a les que estan sotmesos els diferents actius analitzats.
- Una valoració de l'impacte potencial que suposaria per l'organització la materialització de les diferents amenaces a les que estan exposats els diferents actius analitzats.

En la quarta fase, la proposta de projectes, s'han definit un cert nombre de projectes a realitzar els propers tres anys per tal de millorar certs aspectes relacionats amb la Seguretat de la Informació. L'execució d'aquests projectes per part de l'Ajuntament de Riberola ha de permetre, per una banda, millorar el compliment de certs aspectes referents a la norma ISO/IEC 27001, i

per altra banda reduir el possible impacte de la materialització de les amenaces pels actius que presenten més risc. Addicionalment, els diferents projectes poden presentar millores en optimització de recursos o millora de la gestió de processos. Per cadascun dels diferents projectes presentats, s'ha analitzat l'evolució del risc al realitzar-ne la seva execució, així com el seu cost econòmic i la seva duració.

En la cinquena fase s'ha realitzat una auditoria de compliment de l'estàndard ISO/IEC 27002:2005. L'estàndard consisteix en un total de 133 controls o mesures preventives sobre bones pràctiques per a la Gestió de la Seguretat de la Informació. Per cada control s'ha avaluat la seva maduresa o compliment dins l'organització. Aquest estudi ens ofereix un anàlisi de l'estat actual de la seguretat de la informació molt més detallat que el realitzat inicialment mitjançant l'anàlisi diferencial.

Finalment, en la sisena i última fase s'han realitzat els documents necessaris per tal de presentar els resultats i realitzar la pertinent entrega dels informes requerits. En concret s'han elaborat els següents documents:

- Resum executiu
- Memòria descriptiva
- Presentació per la direcció de l'organització
- Vídeo

3. CONCLUSIONS

Amb el Pla de Seguretat elaborat en aquest Treball de Fi de Màster, l'Ajuntament de Riberola disposa de la informació necessària per conèixer i millorar certs aspectes de la Seguretat de la Informació.

Segons l'abast determinat pel projecte en un inici, s'han fixat uns objectius a assolir a llarg plaç, els quals només es poden determinar mitjançant un Pla de Seguretat. Complir aquests objectius permetrà a l'organització un major compliment de la norma ISO/IEC 27001:2005, la creació i gestió d'un Sistema de Gestió de Seguretat de la Informació, la millora de la gestió de la Seguretat de la Informació, els seus processos i el personal associat, així com la fàcil adequació a l'Esquema Nacional de Seguretat.

El seguiment del Pla de Seguretat també ofereix, mitjançant la valoració dels diferents projectes presentats, una ajuda a la direcció de l'organització per tal de centralitzar els esforços en aquelles millores que poden ser més beneficioses per l'organització. En el context econòmic actual, aquest punt és de vital importància, donat que les administracions públiques disposen de recursos econòmics limitats els quals, mal gestionats, poden provocar despeses innecessàries en projectes poc beneficiosos per l'organització. Per tant, proporciona uns objectius a curt i llarg termini per tal que es pugui perseguir i assolir l'estat més òptim possible en la Seguretat de la Informació en les Tecnologies de la Informació i la Comunicació.