Universitat Oberta de Catalunya

Màster Interuniversitari en Seguretat de les TIC (MISTIC)

TREBALL DE FINAL DE MÀSTER

Elaboració d'un Pla de Seguretat de la Informació

Jonatan López Romera

Resum Executiu

TAULA DE CONTINGUTS

1.- Introducció i Motivació

Aquest Treball Final de Màster (TFM) esta orientat a la realització d'un Pla Director de Seguretat (PDS) sobre l'organització seleccionada. El Pla Director de Seguretat té com objectiu establir les bases del procés de **millora contínua** en matèria de seguretat, permetent a les organitzacions conèixer l'estat de la mateixa i plantejar les accions necessàries per minimitzar el impacte dels riscos potencials.

En el nostre cas concret; hem seleccionat una multinacional a nivell europeu del sector de la gran distribució en el sector alimentari, i més concretament; la seva divisió de refrigerats per la regió Ibérica. Aquesta divisió es dedica principalment a la fabricació i comercialització de iogurts i postres pel mercat espanyol i portuguès dintre de la gran distribució amb la incorporació d'un sistema de distribució per poder donar cobertura a la capil·laritat dels "petits comerciants" (tots els punts de comercialització que no es troben agrupats dintre d'un client de gran distribució alimentaria). A la seva vegada, existeix una tercera línia de treball enfocada a la fabricació i comercialització de la "marca blanca" (també anomenada MDD, Marca De Distribució) de les grans ensenyes del sector dintre d'aquest dos països. Dintre de l'apartat 1 de la memòria d'aquest TFM podrem trobar tota la informació detallada de la presentació d'aquest cas d'ús amb la pròpia contextualització i documentació de l'organització sobre la qual desenvoluparem aquest PDS. En aquest mateix apartat, trobarem una descripció de tots els sistemes que trobem presents sobre l'organització i quina es la situació dels mateixos en termes de seguretat de la informació.

Donada l'envergadura de l'empresa, i la dispersió que presenten els diferents sistemes de la informació entre els diferents centres de procés de dades ubicats per tota Europa; cal destacar que aquest PDS estarà enfocat al territori ibèric de la divisió ja que els sistemes que son proveïts des de els centres de procés de dades Internacionals estaran inclosos dintre dels corresponents plans directors dissenyats en els seus països on es troben ubicats. Els proveïdors de l'altre país on es troben ubicats els sistemes, seran els responsables d'incloure sobre els seus plans directors aquests sistemes i garantir la seva seguretat. Per a nosaltres, seran tractats com a serveis extern on només tindrem la responsabilitat de garantir la connexió des de la nostra banda. Per tant, veiem clarament que l'abast sobre el qual buscarem els objectius d'aquest PDS, estarà focalitzat sobre la Regió Ibèrica i els sistemes de la informació que estan establerts dintre d'aquest perímetre d'actuació, i que es proveeixen com a serveis (i estaran classificats com actius del tipus "Servei" dintre de la nostra organització) per a tots els usuaris.

Cal indicar però, que aprofitarem la confecció d'aquest PDS per realitzar la valoració complerta de tots els actius implicats amb els sistemes de la informació de la nostra organització però **ens focalitzarem sobre els serveis oferts als usuaris des de la Regió Ibèrica.**

Un cop realitzada aquesta breu introducció (que trobarem molt més ampliada a l'apartat 1 i 2 de la memòria d'aquest TFM); podem deduir o inclús observar clarament tot una sèrie de beneficis que aporta la realització d'aquest PDS, i que no em d'oblidar que es tracta del punt de partida d'un procés iteratiu i evolutiu en el temps on **l'objectiu principal és millorar constantment en la seguretat de la informació de la nostra societat.** A la seva vegada la confecció del PDS ens permetrà desenvolupar:

- Normes de seguretat organitzatives.
- Pràctiques efectives de gestió de la seguretat.
- Gestió i control sobre les relacions de informació amb terceres organitzacions.
- Complir les diferents conformitats a nivell de la legislació i reglaments aplicables.

Per tant; veiem clarament, que la motivació d'aquest PDS esta orientada principalment en **conèixer** quina es **la situació actual de la nostra organització a nivell de la seguretat de la informació**; en la qual podrem observar clarament quin es l'estat del risc al que es troba exposat actualment l'organització, com també podrem visualitzar quin es l'estat de compliment de l'organització respecte l'ISO / IEC 27002:2005; i un cop conegut l'estat de la seguretat en l'empresa i el nivell de compliment dels controls ISO; estarem en disposició de plantejar projectes a implementar que millorin l'estat de la seguretat en l'organització, que al cap i la fi, busca **l'evolució del nivell de seguretat dels sistemes de la informació.** Aquesta motivació esta supeditada per la intenció clara d'una millora constant de la seguretat com una reducció clara dels riscos als quals s'està exposat.

2.- Objectiu del TFM

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

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

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

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

- Formular els requisits i objectius de seguretat de la informació de la nostra organització.
- Assegurar que els riscos de seguretat es gestionen de manera efectiva en termes de costos.
- Assegurar el compliment de lleis i regulacions vigents.
- Implementar i gestionar els controls necessaris per a assegurar que s'aconsegueixen els objectius de seguretat que ha definit l'organització.

- Definir nous processos de gestió de la seguretat, o identificar i aclarir els processos que ja hi ha.
- Implicar tant la direcció com la resta de departaments de l'organització en l'estat de les activitats de gestió de la seguretat ja que es tracta d'un benefici comú.
- Conèixer el grau de compliment de polítiques, directives i estàndards adoptats per l'organització, per part d'auditors interns o externs.
- Establir polítiques, directives, estàndards o procediments de seguretat de la informació en les relacions amb tercers.
- Convertir la seguretat de la informació en un facilitador del negoci.
- Proporcionar informació rellevant sobre l'estat de la seguretat de la informació a clients.

3.- **Enfocament** del TFM

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

De cara a poder complir aquest objectius:

- Identificarem i valorarem els actius corporatius com a punt de partida mitjançant el corresponent anàlisi de riscos. *(Punt 3 de la memòria)*
- Avaluarem les amenaces i les classificarem. *(Punt 3 de la memòria)*
- Avaluarem el nivell de compliment de la ISO / IEC 27002:2005 en l'organització (tot i no ser obligatòria per no tractar-se d'una empresa pública, es un clar referent per les empreses privades). *(Punt 4 de la memòria)*

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

- Preparar propostes de projectes de cara a aconseguir una adequada gestió de la seguretat i millorar constantment la situació actual. *(Punt 5 de la memòria)*
- Obtenir uns resultats clars que ens permetin presentar-los fàcilment i arribar a la comprensió dels mateixos per part de la pròpia direcció que sol validar les inversions dels projectes futurs. *(Punts 3 y 4 de la memòria)*

Per tant i a mode d'introducció de la memòria d'aquest TFM, podem comentar clarament que s'ha estructurat la confecció d'aquest PDS en les següents fases:

- FASE 1: Contextualització i documentació de l'organització.
- FASE 2: Definició del Objectius del Pla Director.
- FASE 3: Estat del Risc: Identificació i valoració dels actius i amenaces
- FASE 4: Auditoria de compliment de la ISO/IEC 27002:2005
- FASE 5: Propostes de projectes de millora.

4.- Conclusions

Gracies a la confecció d'aquest Pla de Seguretat de la Informació hem pogut observar clarament:

- ✓ La situació actual complerta de risc a la qual ens trobem exposats.
- ✓ El nivell de compliment actual de l'organització a nivell de la normativa ISO/IEC 27002:2005

A la seva vegada, indirectament i degut a la confecció del PDS; per primer cop es té a l'organització un document referencia a nivell de la seguretat de la informació, en qual es troba presents tots els actius relacionats de l'organització, el seu estudi per conèixer la situació de risc a la qual s'està exposat i que permetrà confeccionar plans d'acció per tal de reduir l'impacte d'una possible materialització i per últim el nivell de compliment de l'organització a nivell de la normativa vigent i existent en termes de seguretat de la informació.

Evidentment, l'objectiu de plasmar la situació actual, es clarament un punt de partida de cara a evolucionar i millorar els diferents aspectes a considerar per millorar el nostre nivell de seguretat de la informació però cal indicar que ens serveix com a referència de cara a poder estudiar des de possible millores/projectes a implementar i poder observar clarament, i per anticipat, quin seria el seu impacte sobre la seguretat de la informació dels serveis de la nostra organització com també ens permet plantejar procediments d'actuació en previsió a les possibles adversitats detectades durant la confecció d'aquest PDS. Com veiem clarament, es tant important donar solució "amb anticipació" als possibles problemes que poden sortir a nivell de seguretat de la informació com saber com actuar i estar preparat en cas d'una possible amenaça "materialitzada" que per diferents factors no s'ha pogut minimitzar la seva probabilitat d'ocurrència i per tant estarem preparats per contraatacar-la de la forma més eficient possible dintre de les pròpies possibilitats de l'organització.

En termes de seguretat de la informació, cal destacar, que s'ha de considerar tant important la gestió **proactiva** de la seguretat de la informació, (que ens permet preveure possibles problemes i mitigar-los abans de la seva ocurrència), com la pròpia gestió **reactiva** (que ens permetrà reaccionar de la forma més eficient en cas de problema a nivell de seguretat de la informació).

Com podem observar detalladament sobre la memòria del TFM, s'ha afrontat la confecció d'aquest PDS, en aquesta línia realitzant un anàlisi de riscos detallat de l'organització, un estudi de compliment dels controls establerts per la normativa ISO i per últim un plantejament de diferents projectes e iniciatives a implementar sobre l'organització en les dues línies comentades; **proactivament reduint riscos o incrementant el nivell de compliment** i **re activament plantejant iniciatives per saber com actuar davant les possibles amenaces o catàstrofes** que es poden materialitzar sobre la nostra organització.

Podem afirmar, que la confecció d'aquest PDS, ha estat la base pel procés d'evolució continua de la seguretat de la informació de l'organització que ens permetrà gestionar i mesurar la seguretat de la informació, com iniciar un procés d'evolució continuada en busca de la seva excel·lència.