Pla Director de Seguretat

Ajuntament de Fita Alta

Resum executiu

Juny 2016

Nom Estudiant: Andreu Retamero Pallarès

Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Àrea: Sistemes de Gestió de la Seguretat de la Informació

Nom Consultor: Arsenio Tortajada Gallego
Professor responsable de l'assignatura: Carles Garrigues Olivella
Centre: Universitat Oberta de Catalunya

Data Lliurament: 06/06/2016

Índex

1. Motivació

Qualsevol administració pública, i en particular els ajuntaments, depenen de les Tecnologies de la Informació i les Comunicacions (TIC en endavant) per a poder oferir els serveis que li són propis a la ciutadania. Els seus sistemes TIC han de ser administrats amb diligència i s'han de prendre les mesures necessàries per a protegir-los enfront de danys accidentals o deliberats que puguin afectar la disponibilitat, la integritat, la confidencialitat i l'autenticitat de la informació i dels serveis prestats així com garantir una traçabilitat de les operacions que es realitzen.

Els sistemes TIC han d'estar protegits contra amenaces que, com hem vist, poden incidir en la confidencialitat, la integritat, la disponibilitat i l'autenticitat de la informació i dels serveis. Per a defensar-se d'aquestes amenaces cal desenvolupar eines que s'adaptin al canvis de l'entorn per a garantir la prestació continuada dels serveis.

El Reial decret 3/2010 pel qual s'aprova l'Esquema Nacional de Seguretat (en endavant ENS) i el Reial decret 951/2015 que el modifica especifiquen les mesures mínimes de seguretat exigides que han de seguir les administracions públiques en l'àmbit de l'administració electrònica. Aquestes normes estableixen les bases que han de facilitar la continuïtat dels serveis prestats.

Una aproximació a la implantació de la seguretat en una administració pública podria ser centrar-se exclusivament en l'aplicació de les normes que se li apliquen i en particular de l'ENS. Les normes i recomanacions que el regulen recomanen veure la seguretat com un procés que formi part del cicle de vida dels sistemes TIC. La seva aplicació és basa en la realització d'una anàlisis de riscos i en l'aplicació de les seves salvaguardes articulades en un conjunt de projectes que l'adeqüin als nivells exigibles per la normativa vigent.

També es pot fer una aproximació més àmplia a la seguretat dels sistemes TIC fent la implantació d'un Sistema de Gestió de la Seguretat de la Informació (en endavant SGSI) que segueixi la norma ISO/IEC 27001:2013. Aquest enfocament, incorpora dintre seu el descrit anteriorment per l'ENS però va més enllà ja que un SGSI segons la ISO 27001 "És un sistema de gestió que comprèn la política, l'estructura organitzativa, els procediments, els processos i els recursos necessaris per a implantar la gestió de la seguretat de la informació. Aquest sistema proporciona mecanismes per al control de la seguretat dels actius de la informació i dels sistemes que els processen, en concordança amb les polítiques de seguretat i els plans estratègics de l'organització"

És en aquest context, que la implantació d'un SGSI a l'Ajuntament que segueixi la norma ISO/IEC 27001:2013 és considera una forma efectiva i eficient d'assolir els requisits legals i alhora de garantir que les polítiques de seguretat estan alineades amb els plans estratègics i de negoci de l'organització en el marc d'un sistema de millora contínua de la seguretat.

2. Enfoc del projecte

La metodologia seguida per a la realització del Pla Director ha estat seguir una aproximació per fases al projecte. S'ha contemplat la realització de 6 fases:

- Situació actual : Contextualització, objectius i anàlisi diferencial
- Sistema de Gestió Documental
- Anàlisi de riscos
- Proposta de projectes
- Auditoria de Compliment de la ISO/IEC 2702:2013
- Presentació de resultats i lliurament d'informes

En la primera fase s'han definit les bases del posterior desenvolupament del projecte i s''ha seleccionat l'empresa d'estudi, l'Ajuntament de Fita Alta. Un cop seleccionada l'empresa s'ha realitzat una anàlisi detallada d'aquesta, s'ha definit l'abast del Pla Director de Seguretat i s'ha realitzat una anàlisi diferencial per a comprovar el grau de compliment inicial de la norma 27002:2013.

En aquesta fase ens hem documentat sobre la metodologia de gestió de riscos MAGERIT i la normativa de referència que utilitzarem pel desenvolupament del projecte, la norma ISO/IEC 27001:2013

En la segona fase s'ha desenvolupat tot l'esquema documental necessari per a poder certificar el sistema i que ha de tenir tot Sistema de Gestió de la Seguretat de la Informació (SGSI). Els documents elaborats han estat:

- la Política de Seguretat
- Procediment d'auditories internes
- gestió d'indicadors
- procediment de revisió per la direcció
- gestió de rols i responsabilitats
- metodologia d'anàlisi de riscos
- declaració d'aplicabilitat

En la segona fase s'han establert les metodologies a seguir per a la realització de l'anàlisi de riscos i la l'auditoria de compliment de les fases posteriors.

En la tercera fase s'ha realitzat una anàlisi de riscos seguint la metodologia MAGERIT proposada pel Consell Superior d'Administració Electrònica. Aquesta anàlisi ens ha facilitat:

- la identificació i la valoració dels actius essencials de l'organització
- la definició de les amenaces a les que estan exposats aquests actius
- l'avaluació de l'impacte potencial que suposaria la materialització de les amenaces a les que estan exposats els actius

S'ha utilitzat l'eina EAR-PILAR, desenvolupada pel CCN-CERT, per a fer l'anàlisi de riscos. Aquesta eina utilitza una base de dades d'amenaces amb les probabilitats de materialització d'aquestes sobre el diferents tipus d'actius, la qual cosa permet un càlcul del valor de risc residual avaluant les salvaguardes

aplicades al SGSI. La utilització d'aquesta eina ha facilitat la generació de múltiples informes que s'han utilitzat com a font d'informació per a la realització del Pla Director.

La quarta fase ha estat la definició i planificació d'un conjunt de projectes agrupats en un Pla de Millora amb un doble objectiu:

- la implantació d'un SGSI que segueixi la norma ISO/IEC 27001:2013
- reduir el principals riscos del sistema avaluats a la fase anterior.

El Pla de Millora contempla l'execució dels projectes en dos semestres de forma que al finalitzar l'any s'hagin assolit els objectius de la primera etapa del Pla anomenada "fase objectiu". El Pla Director està dissenyat per a que el SGSI s'acosti en un any al compliment de la norma però no l'assoleixi totalment. Al finalitzar l'any s'ha de fer una revisió de l'anàlisi de riscos i actualitzar la proposta de projectes que ens portarà, en una segona etapa, al compliment de la norma en la seva totalitat.

En la cinquena fase s'ha avaluat la maduresa de la seguretat pel que fa als diferents dominis de control plantejats per la ISO/IEC 27002:2013. S'ha realitzat un "Informe d'auditoria" fent la suposició que s'han implementat tots els projectes definits a la fase anterior. Aquesta fase també ha identificat les No-Conformitats del sistema i això ha permès dissenyar les accions necessàries per a resoldre-les així com implantar les millores recomanades al sistema.

La sisena i última fase ha consistit en la recopilació de tota la informació generada en les fases anteriors per a donar-li el format adequat per a la seva presentació. S'han generat els següents documents:

- Resum executiu
- Presentació de defensa del Treball de Fi de Màster
- Vídeo de defensa del Treball de Fi de Màster
- Memòria del projecte que inclou les tasques de totes les fases realitzades

3. Anàlisi crític de les tasques realitzades

El Pla Director de la Seguretat de la Informació servirà per a que l'Ajuntament de Fita Alta tingui una fulla de ruta que li permeti gestionar d'una forma sistemàtica i adequada la seguretat dels seus sistemes d'informació.

La millor manera de gestionar la seguretat és utilitzar uns estàndards reconeguts internacionalment que garanteixin que es fa un ús correcte dels sistemes d'informació que ajudi a millorar la confiança que els ciutadans tenen en l'administració electrònica.

La realització del Pla Director ha significat treballar la capacitació i els coneixements necessaris per a la implantació d'un SGSI. El mateix procés seguit durant la implantació és similar al que la norma ISO/IEC 27001 proposa per al seu manteniment i millora al llarg del temps. És el que anomenem cicle de Deming o de millora contínua PDCA (**P**lan, **D**o, **C**heck, **A**ct).

Un cop implantat el nostre SGSI haurem fet un cicle sencer i tornarem a estar a la primera fase, la fase **P**lan (de **P**lanificació) on revisarem l'adequació de la Política de seguretat, l'abast del SGSI, les polítiques d'alt nivell i els objectius de seguretat. Un cop revisats aquests punts tornarem a realitzar una anàlisi de riscos i actualitzarem l'avaluació de l'impacte residual que la nostra organització està disposada a assumir. Totes aquestes habilitats i competències les hem treballat a la fase 1 (*Objectius i anàlisi diferencial*), la fase 2 (*Sistema de Gestió documental*) i la fase 3 (*Anàlisi de riscos*) del TFM.

Un cop realitzada la planificació, es passa a la fase **D**o (**F**er) on implantarem un Pla de Gestió del risc com conjunt de projectes agrupats en un Pla de millora de la seguretat. Aquest Pla contemplarà la selecció i implantació d'indicadors que ens permetran gestionar el procés. Aquestes habilitats i competències s'han treballat a la fase 4 del TFM (*Proposta de projectes*).

Implantades les accions del Pla de Millora només cal monitoritzar el procés de la seguretat i revisar-lo de forma regular utilitzant els indicadors definits. Això és el que es fa a la fase **C**heck (Verificar). També es realitzen auditories internes de forma planificada per a fer una validació més exhaustiva del sistema. Les habilitats necessàries per a la realització de les auditories s'han treballat a la fase 5 del TFM (*Auditoria de compliment*).

El tancament del cicle de millora contínua es produeix a la fase **A**ct (Actuar) que és on s'implanten les millores i les accions correctives i preventives que s'han posat de manifest a l'Auditoria interna del SGSI. Aquesta fase no s'ha treballat de forma explícita en el TFM atès que és una part pròpiament centrada en el manteniment del sistema i és complicat treballar-la de forma efectiva en el disseny d'un Pla Director si el SGSI no està implantat i en funcionament.

Analitzada la feina feta durant el TFM hem de valorar si s'han assolit els objectius definits a l'inici del projecte i en cas que no hagi estat així identificar quins han estat els motius que no ho han permès.

Recordem quins eren els objectius del TFM:

- Compliment de la normativa legal en matèria de seguretat: ENS, LOPD
- Implantació de les bones pràctiques en Seguretat dels SGSI definides a les normes ISO/IEC 27000 (27001:2013 com a norma certificable i 27002:2013 com a recull de bones pràctiques)
- Millorar la seguretat dels sistemes de gestió de la informació de l'Ajuntament
- Oferir serveis segurs a la ciutadania
- Millorar la confiança que tenen els ciutadans en l'administració

L'anàlisi de compliment realitzat a la fase 5 (*auditoria de compliment*) a la meitat del procés d'implantació evidencia una millora significativa del SGSI en el compliment de la norma ISO/IEC 27002:2013 així com la possibilitat d'assolir el compliment efectiu en un any vista, tal i com s'havia planificat inicialment. L'alineació en matèria de seguretat entre les normes ISO/IEC i l'ENS fa que la implantació i compliment d'una d'elles millori significativament la implantació i el compliment de l'altra norma.

En aquest sentit podem afirmar que l'avaluació del procés a la meitat de la seva execució és positiva i els dos primers objectius s'estan assolint. Si el procés marcat pel Pla Director segueix el mateix ritme els objectius s'hauran assolit plenament a la finalització del Pla en el termini previst.

Així mateix, en aquests moments ja podem donar per assolit plenament l'objectiu que el SGSI de l'Ajuntament de Fita Alta ha millorat la seva seguretat. L'aplicació del Pla Director, la implantació de la norma ISO/IEC 27001:2013 i els resultats de l'auditoria de compliment així ho corroboren.

S'han assolit la resta d'objectius? Els serveis que s'ofereixen a la ciutadania són segurs? S'ha millorat la confiança que els ciutadans tenen en l'Administració?. Aquests objectius són de difícil mesura ja que impliquen valoracions subjectives.

Sense cap mena de dubte si millorem la seguretat dels nostres sistemes llavors també haurem fet més segur el servei que s'ofereix al ciutadà. Una altra cosa molt diferent és que la ciutadania sigui capaç de percebre aquest canvi. En matèria de seguretat costa molt generar confiança mentre que la materialització dels incidents sempre generarà una sensació d'inseguretat. No hi ha cap recepta que ens porti a l'assoliment de la confiança que no sigui la utilització de les millors pràctiques que els mercat, la legalitat i les normes ens puguin oferir.

Cal analitzar el seguiment de la planificació i la metodologia utilitzada per a la realització del "Pla Director de Seguretat" per a fer-ne una valoració.

En aquest sentit i amb caràcter general, s''ha seguit la metodologia i la planificació del TFM que es van marcar a l'inici del projecte. Val a dir que s'ha fet una variació important en la metodologia. S'ha utilitzat l'eina EAR-PILAR desenvolupada pel CCN-CERT per a fer l'anàlisi de riscos que segueix la metodologia MAGERIT proposada pel Consell Superior d'Administració

Electrònica. Si bé la metodologia proposada pel TFM és la mateixa, la metodologia MAGERIT, el resultat i la forma de fer l'anàlisi de riscos utilitzant les eines EAR-PILAR ha estat diferent de la proposada a les guies del TFM.

Hi ha tres versions de l'eina EAR-PILAR per a fer l'anàlisi de riscos: PILAR, PILAR-Bàsic i μPILAR. Es va optar per la utilització de l'eina μPILAR a la fase 3 (*Anàlisi de riscos*) ja que suposadament permetia fer de forma ràpida l'anàlisi de riscos amb una definició bàsica dels actius.

Això no va ser així. És cert que es va partir d'una definició ràpida dels actius essencials i una enumeració de la resta dels actius segons les seves funcions. En canvi la feina d'avaluació de les salvaguardes que permetia calcular el risc real, residual i de les fases definides al projecte ha estat llarga i feixuga. La documentació de μPILAR parlava de fer-ho en "*hores*" i aquesta tasca ha portat "*dies*" de feina, gairebé una setmana.

La qual cosa ha fet que la tria de μPILAR com a eina d'anàlisi de riscos no hagi estat una bona elecció. L'eina PILAR genera molts més informes que l'eina μPILAR i la seva utilització no aportava un increment significatiu de feina. La tria de l'eina μPILAR, que ara considerem equivocada, ja no va tenir marxa enrere quan es van poder apreciar les mancances que tenia ja que la planificació del TFM estava molt avançada i no permetia fer una nova anàlisi de riscos. Tot i aquest fet, s'ha migrat el projecte de l'eina μPILAR a l'eina PILAR (perdent un parell de dies de feina en adaptacions i revisions) que ha permès que les fases finals del TFM i els informes utilitzats al lliurament final s'hagin generat amb aquesta versió de l'eina.

L'eina PILAR, la més completa de les eines desenvolupades pel CCN-CERT, permet una anàlisi exhaustiva dels actius totalment compatible a la descrita per la metodologia i no és limita als actius essencials (d'informació o serveis), punts d'interconnexió de xarxa i contractes de terceres parts com fa l'eina μPILAR. També permet fer una anàlisi quantitativa que μPILAR no permet i que no s'ha realitzat en el desenvolupament d'aquest Pla Director.

Analitzarem les tasques que s'han de treballar en el futur i que no han estat explorades amb prou detall en aquest "Pla Directors de la Seguretat".

Es detecta una millora associada a les tasques i habilitats relacionades amb la fase **A**ct (Actuar) del cicle PDCA que recomana la norma ISO/IEC 27001:2013. Per a treballar les capacitacions necessàries caldria una nova fase després de la realització de l'auditoria que comportés l'aplicació de les millores proposades i això queda fora de lloc en un Pla Director. Aquesta fet implica que aquestes habilitats i tasques s'hauran d'assolir fora del marc del TFM.

L'obligació del compliment dels terminis en la redacció del "Pla Directors de seguretat" ha fet que la definició d'alguns inventaris sigui millorable i s'hagi d'anar perfeccionant en les successives iteracions del nostre cicle de millora contínua de la gestió de la seguretat dels sistemes d'informació. Entre aquests inventaris en podríem destacar el detall dels indicadors implantats en l'SGSI i l'inventari d'actius.

4. Conclusions

Per finalitzar, farem un recull de les principals conclusions extretes de la realització d'aquest Treball de Final de Màster i de l'elaboració del "Pla Director de Seguretat".

La primera conclusió és que s'han assolit de forma satisfactòria els objectius plantejats a l'inici del projectes.

La segona conclusió és que l'elaboració del Pla Director, a banda d'oferir una fulla de ruta per a la millora de la seguretat a l'Ajuntament de Fita Alta, també ha servit per a adquirir la capacitació i els coneixements necessaris per a la gestió, manteniment i millora al llarg del temps d'un SGSI basat en la norma ISO/IEC 27001:2013.

La tercera conclusió és que l'auditoria de compliment posa de manifest que el SGSI de l'Ajuntament de Fita Alta ha millorat considerablement des de d'inici de l'aplicació del Pla Director. És de preveure que en una nova iteració del cicle PDCA d'una durada de 12 mesos s'assoleixin els nivells de compliment de la norma ISO/IEC 27001:2013 i de la normativa legal en matèria de seguretat: ENS i LOPD.

La quarta conclusió fa referència a la utilització de les eines de gestió de riscos EAR-PILAR del CCN-CERT. Si és possible, és recomanable fer-les servir ja que aporten molts més beneficis que inconvenients per al manteniment del sistema al llarg del temps. Això si, és recomana fer servir l'eina complerta, PILAR, ja que permet una aplicació total de la metodologia MAGERIT.

La última conclusió que ha posat en evidència la realització d'aquest treball és que la gestió de la seguretat dels sistemes d'informació és un procés i no una tasca. No és la implantació d'un producte o servei, és la implantació d'un procediment de gestió que s'ha d'anar monitoritzant de forma permanent, avaluant els seus resultats per a detectar possibles problemes i corregir-los i on s'han de revisar sempre els objectius, l'abast, les polítiques i criteris aplicats per a millorar-los i adequar-los a la realitat de la nostra organització. Així per a la resta dels anys, en un procés sense fi que el que pretén és anar perfeccionant-se a ell mateix de forma progressiva.