PLAN DIRECTOR DE SEGURIDAD DEL AYUNTAMIENTO DE BUENAS MANERAS

RESUMEN EJECUTIVO

TRABAJO FINAL DE POSGRADO

JUNIO 2017

DIRECTOR: Carles Garrigues

CONSULTOR: Arsenio Tortajada

ALUMNO: Jennifer Gil

Universitat Oberta de Catalunya

POSGRADO EN GESTIÓN Y AUDITORÍA DE LA SEGURIDAD INFORMÁTICA
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

ÍNDICE

1. MOTIVACIÓN DEL PROYECTO.....1
2. ENFOQUE DEL PROYECTO…….....2
3. CONCLUSIONES.....4

1. MOTIVACIÓN DEL PROYECTO

Este proyecto ha sido un reto para mi dado que actualmente estoy trabajando en una empresa de gestión y asesoramiento de seguridad de la información en la cual llevo medio año y he ido plasmando los conocimientos que adquiría en el posgrado en mi día a día laboral y viceversa.

Actualmente, muchas organizaciones y empresas consideran la información como uno de sus valores más importantes. Esto es así porque la disponibilidad, integridad, confidencialidad y autenticidad de esta información, junto con los procesos y elementos que la tratan, siendo vitales e indispensables para el funcionamiento y supervivencia de estas empresas y organizaciones.

Las administraciones públicas, al igual que las empresas y organizaciones, dependen cada vez más de las tecnologías de la información y la comunicación para realizar sus funciones, ya sean relacionadas con los servicios a la ciudadanía o con otras administraciones, entidades o empresas.

Mediante la ejecución de este proyecto, el Ayuntamiento de Buenas Maneras (ayuntamiento inventado) desea implantar un Plan de Seguridad para alcanzar principalmente los tres siguientes objetivos:

- Obtener una visión del estado actual de la seguridad en las Tecnologías de la Información y la Comunicación.

- Proporcionar medidas o actuaciones a realizar a corto o largo plazo para mejorar los aspectos críticos que se detecten, siguiendo unos objetivos concretos y definidos.

- Sentar las bases para la creación de un Sistema de Gestión de Seguridad de la Información (SGSI), para controlar la evolución de la seguridad de la organización a lo largo del tiempo.

Adicionalmente, al tratarse de una administración pública, se requiere el cumplimiento, entre otros, del Esquema Nacional de Seguridad (ENS), el cual prácticamente obliga a disponer de un Sistema de Gestión de Seguridad de la Información.

Existen ciertas metodologías o normas para asegurar que las organizaciones tienen en consideración el estado actual y la evolución de la seguridad de la información, así como de los elementos tecnológicos o físicos con los que interactúa.

El actual proyecto consiste en la creación de un Plan Director de Seguridad utilizando como marco estándar de referencia la norma ISO / IEC 27001 (proveniente de la ISO 17799) y la ISO / IEC 27002, donde se tratan requisitos y códigos de buenas prácticas en la gestión de la seguridad de la información ("information technoloy - Security techniques - Code of pratice for information security management"). Estas buenas prácticas son aptas para cualquier tipo de empresa u organización.

2. ENFOQUE DEL PROYECTO

La realización de este proyecto se ha dividido en las siguientes fases:

- Contextualización, objetivos y análisis diferencial.
- Sistemas de gestión documental.
- Análisis de riesgos.
- Propuesta de proyectos
- Auditoría del cumplimiento
- Presentación de los resultados

En una primera fase, se han definido los principales objetivos del Plan Director de Seguridad, se ha determinado el alcance y se ha realizado un análisis diferencial donde se valora la situación actual de los diferentes puntos de la ISO / IEC 27001 en el Ayuntamiento de Buenas Maneras. Por lo tanto, se analizarán las diferentes medidas y procedimientos de seguridad, así como normativas existentes en relación a la Seguridad de la Información.

En la siguiente fase, se han desarrollado y generado los documentos básicos y algunas plantillas necesarias para la adaptación a la norma ISO / IEC 27001. Como parte principal, se desarrolla el sistema de gestión documental, definiendo la gestión de indicadores, el procedimiento de auditorías internas, la política de seguridad, la metodología de análisis de riesgos y la declaración de aplicabilidad.

El análisis de riesgos llevado a cabo en la tercera fase nos aporta:

- Un análisis detallado de los activos más esenciales relacionados con la Seguridad de la Información.
- Un estudio de las posibles amenazas a las que están sometidos los diferentes activos analizados.
- Una valoración del impacto potencial que supondría para la organización la materialización de las diferentes amenazas a las que están expuestos los diferentes activos analizados.

El análisis se ha basado en la ejecución del análisis de riesgos en la metodología propuesta a Magerit.

En la cuarta etapa se desarrollan los proyectos que contemplan la implantación de los distintos controles destinados a alcanzar los objetivos establecidos en el SGSI.
De este modo, el Ayuntamiento se permite reducir el nivel de riesgo actual y con ello mejorar el estado de seguridad de la organización.
Por consiguiente, se ha trabajado sobre el conjunto de salvaguardas propuestas proporcionando una guía en su implantación.
Se ha utilizado la herramienta PILAR, la cual clasifica la información de salvaguardas según el tipo de protección en el que se hallen enfocadas, por otra según la vinculación a cada uno de los activos en concreto y, por último, según su relación con los controles de la norma ISO 27002:2013.

En la quinta fase se ha realizado una auditoría de cumplimiento del estándar ISO / IEC 27002:2013 tras haber realizado el análisis de riesgos del Ayuntamiento. De este modo, se permite reducir el nivel de riesgo actual y con ello mejorar el estado de la seguridad de la organización.
Llegados a esta fase, se conocen los activos de la empresa y se han evaluado las amenazas. En este punto se evalúa hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad.

Finalmente, en la sexta y última fase se han realizado los documentos necesarios para presentar los resultados y realizar la pertinente entrega de los informes requeridos. En concreto se han elaborado los siguientes documentos:

- Resumen ejecutivo

- Memoria descriptiva

- Presentación por la dirección de la organización

- Vídeo

3. CONCLUSIONES

Con el Plan de Seguridad elaborado en este Trabajo de Final de Posgrado, el Ayuntamiento de Buenas maneras dispone de la información necesaria para conocer y mejorar ciertos aspectos de la Seguridad de la Información.

Según el alcance determinado por el proyecto en un inicio, se han fijado unos objetivos a alcanzar a largo plazo, los cuales sólo se pueden determinar mediante un Plan de Seguridad. Cumplir estos objetivos permitirá a la organización un mayor cumplimiento de la norma ISO /27002, la creación y gestión de un Sistema de Gestión de Seguridad de la Información, la mejora de la gestión de la Seguridad de la Información, los sus procesos y el personal asociado, así como la fácil adecuación al Esquema Nacional de Seguridad.

El seguimiento del Plan de Seguridad también ofrece, mediante la valoración de los diferentes proyectos presentados, una ayuda a la dirección de la organización a fin de centralizar los esfuerzos en aquellas mejoras que pueden ser más beneficiosas para la organización. En el contexto económico actual, este punto es de vital importancia, dado que las administraciones públicas disponen de recursos económicos limitados que, mal gestionados, pueden provocar gastos innecesarios en proyectos poco beneficiosos para la organización. Por lo tanto, proporciona unos objetivos a corto y largo plazo para que se pueda perseguir y alcanzar el estado más óptimo posible en la Seguridad de la Información en las Tecnologías de la Información y la Comunicación.