Resumen ejecutivo
TurisTech Balear SL

Proceso de adecuación de la seguridad de la información en una pequeña empresa

Nombre estudiante: José Sureda Uceda

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre consultor: Arsenio Tortajada Gallego

Centro: Universitat Oberta de Catalunya

Fecha de entrega: 20 de diciembre 2019

Índice

1. Introducción

Como alumno del *Máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones* impartido por la Universitat Oberta de Catalunya, presento el *Resumen Ejecutivo* correspondiente al Proyecto Fin de Máster, a partir de ahora TFM, que responde a la necesidad de implantar un Sistema de Gestión de Seguridad de la Información o SGSI, en la empresa TurisTech Balear SL.

2. Contexto

En la actualidad, es difícil encontrar empresas donde su modelo de negocio no se sustente en sistemas y dispositivos informáticos. Esto ha provocado que la información que se procesa, transmite y almacena en los equipos, se haya convertido en un activo vital para la existencia y funcionamiento normal de sus negocios. Además, las leyes vigentes obligan a las empresas y organizaciones a garantizar la seguridad de ciertos datos.

Un incidente de seguridad en la información puede provocar, entre otras cosas, interrupciones en los servicios, en la producción o incumplir alguna ley, acarreando pérdidas económicas y daños en la imagen corporativa. En el peor de los casos, incluso es posible que se produzca el cierre temporal o completo del negocio.

Estudios recientes indican que las pequeñas empresas son las que menos invierten en seguridad de las TIC, lo cual genera situaciones de riesgo que causan, ya sea de forma intencionada o por accidente, que la información crítica del negocio pueda verse afectada por un incidente.

3. Motivación del proyecto

Educar y concienciar en materia de seguridad de la información son la clave para que las pequeñas empresas afronten con las mejores garantías, los riesgos a las que están expuestas.

A partir de un caso real en una pequeña empresa, este proyecto muestra el proceso completo para implantar un SGSI. Los resultados, al ser veraces, podrán ser tomados como ejemplo de aplicación en otras empresas.

La entidad objeto de estudio se llama de forma ficticia TurisTech Balear SL, la cual es una pequeña empresa tecnológica que ofrece distintos servicios en el sector turístico. Sus activos de información resultan esenciales para el buen funcionamiento del negocio, sin embargo muchos aspectos de la organización no reciben la adecuada atención en relación a la seguridad de la información, por lo que existen riesgos que deben ser gestionados.

4. Objetivos

Se describen parte de los objetivos a alcanzar y que pueden consultarse por completo en la memoria del TFM.

4.1 Generales

- Concienciar a las microempresas y PYMES para que integren la seguridad de la información en su modelo de negocio, evitando tratarla como una cuestión que afecte sólo a ciertos departamentos o proyectos.

- Educar sobre los beneficios que puede aportar a las empresas y organizaciones la implantación de un Sistema de Gestión de Seguridad de la Información.

4.2 Específicos

- Dar a conocer el estado inicial y final de TurisTech Balear en relación a la seguridad de la información.

- Implantar en la empresa una metodología para gestionar los riesgos.

- Obtener una lista de proyectos que la organización deberá desarrollar para situar el estado inicial de seguridad a los niveles definidos en el Plan Director.

- Realizar una auditoría interna de cumplimiento.

5. Metodología

Los objetivos definidos se han conseguido usando estándares y metodologías reconocidas a nivel internacional, en concreto, el proyecto se fundamenta en la norma ISO/IEC 27001:2013, el estándar ISO/IEC 27002:2013, el marco de trabajo MAGERIT, el Ciclo de Deming y el Modelo de Madurez de la Capacidad.

Para llevar a cabo la implantación del SGSI se ha diseñado un Plan Director de Seguridad, el cual contempla todas las tareas necesarias para desplegar el sistema de forma exitosa. Estos cometidos se han distribuido en diversos proyectos que se ejecutaran a corto, medio y largo plazo, en el término de tres años. De forma resumida se indican sus costes anuales de cada período:

- Primer año: 13.200 €
- Segundo año: 9.650 €
- Tercer año: 2.500 €
- **Total: 25.350€**

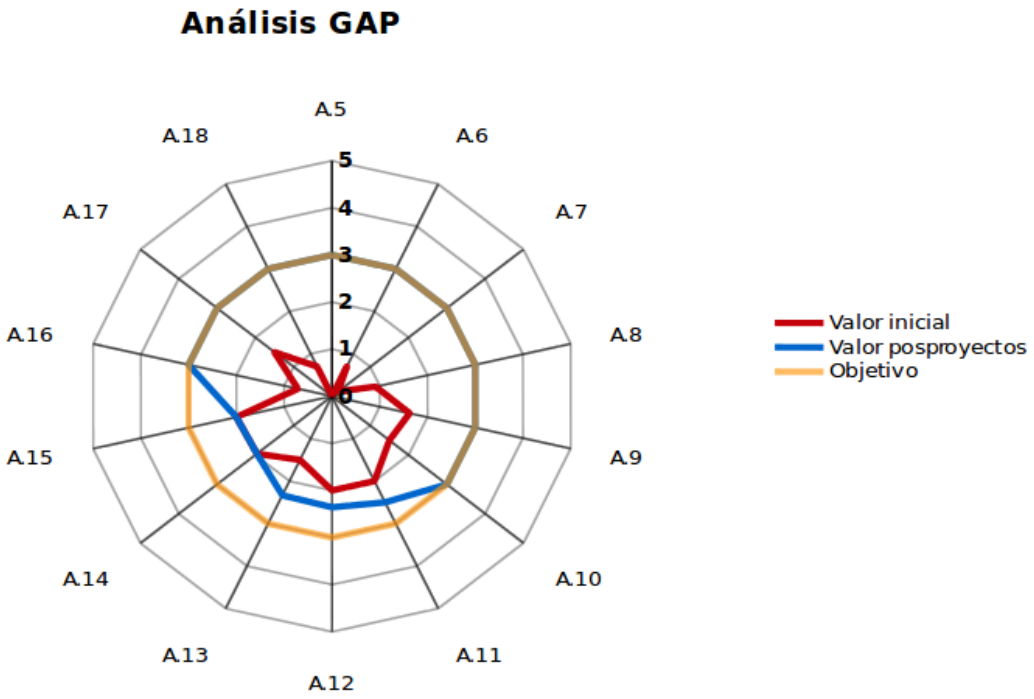
6. Conclusiones

Las previsiones que se obtendrán al finalizar el proyecto lo convierten en una de las mejores opciones para garantizar que TurisTech Balear adquiera, a nivel global, el nivel adecuado de seguridad en sus activos de información. Pasando a ser una empresa mucho más segura y con mayor potencial de reacción ante un incidente de seguridad.

Los servicios prestados y los procesos internos se ejecutarán de forma más eficaz y eficiente, mejorando de esta forma la producción. En consecuencia, se ofrecerá una imagen más profesional y de confianza hacia los clientes. Todos estos avances finalmente compensarán los costes de ejecución del Plan Director de Seguridad.

Para terminar se muestran algunos ejemplos de las previsiones de mejora, pudiéndose consultar con mayor detalle en la memoria del proyecto.

Comparativa del estado inicial y final de la seguridad de la información:



Comparativa inicial y final en relación al cumplimiento de las distintas áreas de la norma ISO/IEC 27002:

Capítulo	Valoración inicial	Valoración posproyectos
5 Políticas de seguridad de la información	0 %	90 %
6 Organización de la seguridad de la información	14,5 %	90 %
7 Seguridad relativa a los recursos humanos	1,7 %	90 %
8 Gestión de activos	16,7 %	90 %
9 Control de acceso	38 %	90 %
10 Criptografía	30 %	90 %
11 Seguridad física y del entorno	50 %	70 %
12 Seguridad de las operaciones	55,4 %	68,57 %
13 Seguridad de las comunicaciones	37,5 %	67,1 %
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	48,3 %	48,3 %
15 Relación con proveedores	50 %	50 %
16 Gestión de incidentes de seguridad de la información	7,1 %	90 %
17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	30 %	90 %
18 Cumplimiento	13 %	90 %

Comparativa del estado inicial y final de los activos de información en relación al umbral de riesgo permitido (no se muestran todos los activos disponibles).