Plan de mejora de la Seguridad de la Información, a través de la implantación de un SGSI

Informe Ejecutivo

Nombre Estudiante: Carlos Vila Martínez
Programa: Proyecto Final de Posgrado Gestión y Auditoría de la Seguridad
Nombre Consultor: Arsenio Tortajada Gallego
Centro: Universitat Oberta de Catalunya
Fecha Entrega: 7 de Junio de 2017

Introducción

El presente proyecto versa sobre la implantación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** en FCA, una empresa familiar fundada en el año 1967 y dedicada al sector de la Ferretería y Suministro Industrial.

Nos situamos en un contexto de empresa madura y asentada en el mercado, que dispone de un sistema de información automatizado desde hace más de 30 años. Pese a ello, su seguridad no ha evolucionado como debiera y tiene serias carencias que deben ser abordadas.

Las circunstancias comerciales actuales han llevado a la gerencia de la organización a implicarse profundamente en el proyecto y plantearse la implantación de un SGSI, recurriendo a parte del personal externo que actualmente da soporte técnico.

Con la implantación de este SGSI se pretende **sentar las bases** para llevar a cabo una **mejora continua** en lo que a **seguridad de la información** se refiere y adicionalmente llegar a disponer de un sistema que pueda ser certificado bajo la Norma ISO/IEC 27001:2013.

La implantación de este **SGSI** aportará a FCA una serie de **beneficios** entre los que se pueden destacar:

- Reducción de riesgos de pérdida de información para la empresa.
- Revisión periódica de todos los riesgos a los que está expuesta.
- Incorporación de una metodología clara para gestionar la seguridad.
- Implantación de medidas de seguridad para la empresa y sus clientes.
- Identificación y registro de incidencias para una mejora continua de la seguridad en la organización.
- Un SGSI otorga una garantía de seguridad ante clientes y socios.
- Permite disponer de un plan de contingencia para poder seguir operando con normalidad ante un incidente de seguridad.
- Garantiza que la empresa está cumpliendo con la legislación vigente.
- Dota a la empresa de una ventaja competitiva frente a sus clientes, incrementando su imagen a través de un entorno seguro.
- Permite a la empresa certificarse en la ISO27001, norma internacional de referencia en cuanto a seguridad de la información se refiere.

FCA dispone de una estructura jerárquica muy básica, en la que gran parte de los roles y funciones son compartidos por todos los miembros de la organización.

El proyecto de implantación de este SGSI se ha llevado a cabo a través de los siguientes Hitos:

Hito 1: Análisis de la situación actual de la empresa FCA

En esta primera fase del proyecto se han realizado las siguientes tareas:

- **Enfoque y selección de la empresa**: se ha escogido una empresa familiar de pequeña dimensión con un sistema de información

implantado hace 30 años pero en un estado muy inicial de madurez, en cuanto a seguridad de la información se refiere.

- **Objetivos del Plan Director de Seguridad**: para la consecución del presente proyecto se deben alcanzar los siguientes 5 objetivos:
  - Implantación del SGSI.
  - Actualización y ampliación de la red corporativa.
  - Creación de un plan de contingencia ante desastres, para garantizar la continuidad de negocio.
  - Optimización del ERP que está en funcionamiento actualmente.
- **Análisis diferencial**: Partimos del estado inicial en el que se encuentra el sistema de información y hacemos una valoración (análisis diferencial) de las medidas de seguridad que están implantadas en ese momento.

Hito 2: Elaboración del Sistema de Gestión Documental

En esta segunda fase del proyecto hemos sentado las bases del Sistema de Gestión Documental del futuro SGSI, que contendrá:

- **Política de Seguridad de FCA (Anexo I)**: Este documento, inexistente hasta la fecha, contiene unos principios generales, las responsabilidades de cada empleado en cuanto a seguridad de la información se refiere y el conjunto de normas aplicables sobre los activos de la empresa que están relacionados con el sistema de información.
- **Procedimiento a seguir durante las Auditorías Internas (Anexo III)**: en este documento se ha establecido el alcance y objetivo que deben tener las auditorías periódicas, así como la fecha y lugar para realizarlas. Finalmente se ha fijado quien estará presente en las mismas, tanto por parte del equipo auditor como de FCA. Estas auditorías internas se regirán por los criterios contemplados en la Norma ISO/IEC 27001:2013.
- **Gestión de Indicadores (Anexo IV)**: Se han desplegado un total de 24 indicadores para medir la eficacia de los controles de seguridad implantados.
- **Procedimiento de Revisión por parte de la Dirección (Anexo V)**: Se han definido un total de 9 tareas que la dirección debe llevar a cabo para la revisión y mejora continua del SGSI.
- **Gestión de Roles y Responsabilidades (Anexo VI)**: Se ha definido un total de 4 roles asociados a las 4 áreas de la empresa. Para cada uno de ellos se han establecido una serie de responsabilidades en cuanto a gestión de la seguridad de la información.
- **Metodología de Análisis de Riesgos**: Se ha adoptado la metodología *Magerit* para el análisis y tratamiento de los riesgos en la empresa FCA.
- **Declaración de Aplicabilidad (Anexo X)**: Punto de partida para determinar las áreas de mejora en seguridad de la información según Norma ISO/IEC 27002:2013.

Hito 3: Análisis de Riesgos

La tercera fase del proyecto ha consistido en la realización de un análisis del riesgo existente en la organización, a través de las siguientes tareas:

- **Inventario de activos (Anexo I)**: Se ha realizado un inventario de todos los activos relacionados con el sistema de información en los siguientes ámbitos:
  - *Instalaciones*: Se han registrado un total de 6 activos, distribuidos en dos sedes y un vehículo.
  - *Hardware*: Se han registrado un total de 9 activos, distribuidos en 1 servidor, equipos fijos, portátiles, impresoras, dispositivos móviles y otro hardware.
  - *Aplicaciones*: Se han registrado un total de 8 activos, distribuidos en ERP, sistemas operativos, ofimática, comunicaciones y seguridad.
  - *Datos*: Se han registrado un total de 3 activos, distribuidos entre bases de datos y resto de información (digital y en formato papel).
  - *Red*: Se han registrado un total de 5 activos, distribuidos entre servicios de voz, datos, LAN y WIFI.
  - *Servicios*: Se han registrado un total de 7 activos, correspondientes a diferentes servicios del sistema de información.
  - *Equipamiento auxiliar*: Se han registrado un total de 5 activos, distribuidos entre equipos de climatización, cableado, mobiliario y seguridad.
  - *Personal*: Se han registrado un total de 5 activos, distribuidos en operadores internos, operadores externos, soporte TIC externo, clientes y proveedores.
- **Valoración de Activos (Anexo I)**: Se han definido las 5 dimensiones de seguridad de la información y procedido a valorar (escala del 0 al 10) cada uno de los activos en función del daño que provocaría a la organización un incidente de seguridad en el que dicho activo estuviese involucrado.
- **Identificación y Análisis de Amenazas (Anexo VII)**: Para la realización de esta fase se ha utilizado la metodología Magerit y clasificado las 31 posibles amenazas en 5 grupos según el origen de las mimas, es decir, de; origen natural, origen humano (intencionadas), del entorno, sobre el hardware/software, origen humano (no intencionadas) y otras amenazas.
- **Análisis del riesgo (Anexo VIII)**: Partimos de la relación de activos identificados y de las amenazas, en función de las dimensiones ACIDT, para posteriormente determinar la probabilidad de ocurrencia de la misma. Llegados a este punto analizamos el impacto provocado por la materialización de la misma y determinamos el riesgo, aceptable y residual, observado en cada uno de los 8 ámbitos contemplados.

Hito 4: Propuestas de Proyectos

Una vez identificadas las principales amenazas y determinado el riesgo e impacto derivado de la materialización de las mismas, se han presentado las siguientes 8 propuestas de proyectos para la mejora integral de la seguridad de la información:

- **PPT-01-INS**: Proyecto de mejora para la seguridad de las instalaciones.
- **PPT-02-HDW**: Proyecto de mejora para la seguridad del hardware.
- **PPT-03-APP**: Proyecto de mejora para la seguridad de las aplicaciones.
- **PPT-04-DTS**: Proyecto de mejora para la seguridad de los datos.
- **PPT-05-NTW**: Proyecto de mejora para la seguridad de la red.
- **PPT-06-SRV**: Proyecto de mejora para la seguridad de los servicios.
- **PPT-07-AUX**: Proyecto de mejora de seguridad en equipamiento auxiliar.
- **PPT-08-PRS**: Proyecto de mejora de seguridad en el personal.

Cada una de estas propuestas lleva aparejada una estimación económica y una previsión temporal.

Finalmente se presentamos un diagrama con la evolución, desde el estado inicial hasta la implantación de estos proyectos, sobre cada uno de los dominios de la ISO27001:2013.

Hito 5: Auditoría de cumplimiento

La última fase del primer ciclo del SGSI ha consistido en la realización de una auditoría interna de cumplimiento, tomando como base los 14 dominios y 114 controles de la ISO/IEC 27002:2013. El resultado final nos aporta un total de 6 no conformidades encontradas, clasificadas en:

- **No Conformidades Menores** que deben ser resueltas en un plazo no superior a los 6 meses y que han afectado a los siguientes dominios:
  - *NC-01 → Dominio afectado → A.7 Seguridad relativa a los RRHH.*
  - *NC-02 → Dominio afectado → A.9 Control de acceso.*
  - *NC-03 → Dominio afectado → A.11 Seguridad física y del entorno.*
  - *NC-04 → Dominio afectado → A.12 Seguridad de las operaciones.*
- **No Conformidades Mayores** que deben ser resueltas de forma inmediata y que han afectado a los siguientes dominios:
  - *NC-05 → Dominio afectado → A.13 Seguridad comunicaciones.*
  - *NC-06 → Dominio afectado → A.16 Gestión incidentes seguridad.*

Conclusiones

Partimos de un estado inicial en el que la empresa FCA se encuentra bien asentada en el mercado y con un sistema de información mixto implantado hace más de 30 años. La implantación del presente SGSI dota a FCA de las

medidas de seguridad necesarias para garantizar una reducción considerable de los riesgos y amenazas detectadas en el desarrollo de este proyecto.

Se ha realizado un **inventario y valoración de activos**, para posteriormente llevar a cabo una primera valoración del estado de su seguridad. A continuación se ha procedido a una **identificación y valoración** de las posibles **amenazas**, analizando el **riesgo** e impacto de materialización de las mismas ante un eventual incidente de seguridad.

Una vez obtenidos y evaluados los resultados anteriores, se plantean una serie de **propuestas de proyectos** para la mejora de la seguridad de la información. Dichos proyectos llevan aparejados, además de unas medidas de mejora, una previsión temporal y una estimación económica.

Finalmente se realiza la **auditoría interna** en base a los 14 dominios y 114 controles de la Norma ISO/IEC 27002:2013. Esto da como resultado una serie de “no conformidades” que deben ser resueltas en los plazos establecidos.

A partir de este momento comienza el **segundo ciclo PDCA** (Plan-Do-Check-Act) del **Sistema de Gestión de Seguridad de la Información** implantado en FCA.