Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001

Trabajo final de carrera

Manuel Muñoz Martín

Área de Gestión de proyectos
Universitat Oberta de Catalunya
Tutor Ana Cristina Domingo Troncho

Junio, 2015

La norma ISO 27001

- Interés y motivación en el desarrollo del trabajo orientado al aprendizaje y formación sobre la norma ISO 27001.
- La elección de esta norma es debido a que se trata de un estándar internacional en seguridad de la información ampliamente reconocida.
- La norma se basa en el Ciclo de Deming y a partir de esta desarrollaremos la implantación del proyecto.
- El proyecto se compone de tres partes bien diferenciadas:
  - Análisis
  - Implantación
  - Conclusiones

Parte I. Análisis

- Definimos los objetivos de negocio que persigue la implantación de la norma.
- Realizamos un análisis de situación de la empresa Treval de nuestro trabajo y especificamos claramente el alcance de nuestro proyecto.
- Realizamos un análisis diferencial aunque no sea obligatorio por parte de la norma.
- Definimos las políticas de seguridad y el enfoque de análisis de riesgo.
- Realizamos el inventario y valoración de los activos de nuestra empresa.
- Especificamos la valoración de los riesgos y redactamos la declaración de aplicabilidad de la norma.

Objetivos de negocio

- Previamente a las demás tareas se debe realizar un análisis de cuáles son los objetivos de negocio que persigue la adopción de la norma.
- Estos objetivos pueden provenir de diferentes ámbitos de una empresa y no tienen por qué estar ligados a un área determinada.
- Cada uno de estos objetivos puede variar dependiendo del sector empresarial o nivel organizativo.

Descripción de la empresa

- Realizaremos un análisis de la empresa para saber su situación actual y funcionamiento.
- El análisis organizativo es necesario para poder saber su gestión de procesos interna.
- El análisis de su infraestructura tecnológica nos ayudará a saber su grado de compromiso con las tecnologías de la información.

Alcance de proyecto

- Debemos definir en esta fase los límites del proyecto y hasta donde abarcaremos.
- El alcance puede afectar a una parte o toda una organización.
- También podemos definirlo a partir de procesos o unidades organizativas.
- Definir de manera errónea o arbitraria el alcance del proyecto puede llevar a un aumento del tiempo o recursos para el desarrollo del mismo.

Análisis diferencial (Gap Analysis)

- Aunque no sea obligatorio por parte de la norma realizar un análisis diferencial previo nos revelará la situación actual de la empresa respecto a la norma ISO 27001.
- Utilizaremos el documento de aplicabilidad como base para hacer el estudio.

Objetivos	Observaciones	Cumple	Justificación
6.2 Terceras partes			
6.2.1 Identificación de los riesgos relacionados con las partes externas	Hay informes de riesgos derivados de los procesos externos.	Parcial	
6.2.2 Consideraciones de la seguridad cuando se trata con los clientes		Parcial	
6.2.3 Consideraciones de la seguridad en los acuerdos con terceras partes	Existen contratos de confidencialidad.	Si	

Políticas de seguridad y enfoque del análisis de riesgos

- Debemos definir las políticas de seguridad de la organización.
- Se basarán en las directrices de la empresa en materia de seguridad.
- Seleccionaremos la metodología de evaluación de riesgos para el proyecto entre todas las alternativas.
- Utilizaremos Magerit para realizar el análisis de riesgos creada por el Consejo Superior de Administración Electrónica.

Inventario de activos

- Hacemos una lista con todos los activos definidos en el alcance asignándoles responsables, categorías y ubicaciones.
- Este documento nos servirá para saber los riesgos expuestos en la organización.

Datos de desarrollo	Control de código fuente, versiones, bases de datos, etc	Datos	Sistemas	Responsable de Sistemas
Correo electrónico	Datos de Mail	Datos	Sistemas	Responsable de Sistemas
Claves digitales	VPN, PGP, SSL, etc	Claves criptográficas	Sistemas	Responsable de Sistemas
S.O	Sistemas operativos	Aplicación	Sistemas	Responsable de Sistemas
Antivirus	Sistemas de seguridad	Aplicación	Sistemas	Responsable de Sistemas
App. de desarrollo	Software privativo de desarrollo	Aplicación	Sistemas	Responsable de Sistemas
Switch	Armario para toda la empresa	Hardware	Sistemas	Responsable de Sistemas
Backup	Sistemas de backup	Auxiliar	Sistemas	Responsable de Sistemas
Internet	Conexión a internet	Redes	Sistemas	Responsable de Sistemas
Red ethernet	Red de comunicación de la empresa	Redes	Sistemas	Responsable de Sistemas
CPD empresa	Sistema con SAI, sistema antiincendios, etc	Instalaciones	Sistemas	Responsable de Sistemas

Valoración de activos

- Realizamos una valoración de los activos a partir de su confidencialidad, integridad y disponibilidad.
- La suma de estos valores nos dará el valor del activo en la organización respecto a la seguridad de la información.

Activo	Conf.	Int.	Disp.	Total
Servidores de Sistemas	2	3	4	**9**
Router	1	1	4	**6**
Cortafuegos	1	1	4	**6**
Equipos PC de desarrollo	1	2	3	**6**
Impresoras	1	1	4	**6**
Servicios cloud	2	4	4	**10**
Datos de desarrollo	4	4	1	**9**
Correo electrónico	4	4	2	**10**
Claves digitales	4	4	1	**9**
S.O	2	2	2	**6**
Antivirus	2	2	3	**6**
App. de desarrollo	2	2	2	**6**
Switch	1	1	4	**6**
Backup	3	3	3	**9**
Documentación	4	2	1	**7**
Internet	3	3	3	**9**
Red ethernet	3	3	3	**9**
CPD empresa	4	4	4	**12**
Personal	1	2	3	**6**

Identificación de amenazas y valoración de riesgos

- Identificamos del listado de amenazas de la metodología Magerit aquellas que más afectan a nuestros activos.
- El nivel de riesgo total se calcula a partir de multiplicar los valores de impacto, amenaza y vulnerabilidad.

Activo	Amenaza	Impacto	Nivel de amenaza	Vulne.	Nivel de riesgo
Servidores de Sistemas	Errores de usuario	9	2	3	54
Router	Fallo de comunicaciones	6	3	3	54
Cortafuegos	Fallo de comunicaciones	6	3	3	54
Equipos PC de desarrollo	Errores de usuario	6	2	3	36
Impresoras	Error de mantenimiento	6	2	2	24
Servicios cloud	Fallo de comunicaciones	10	3	2	60
Datos de desarrollo	Robo	9	3	3	81
Correo electrónico	Fallo de comunicaciones	10	2	2	40
Claves digitales	Robo	9	2	3	45
S.O	Error de mantenimiento	6	2	3	36
Antivirus	Error de mantenimiento	6	2		36
App. de desarrollo	Fallo de software	6	3	3	54
Switch	Fallo de comunicaciones	6	2	2	24
Backup	Errores de usuario	9	2	2	36
Documentación	Fuego	7	2	2	28

Documento de aplicabilidad

- Con el análisis de riesgos ya podemos saber cuáles son los controles a implementar en la empresa.
- El documento de aplicabilidad se corresponde con el anexo A de controles de la norma.

Objetivos	Aplicable	Justificación
6. Organización de la seguridad de la Información		
6.1 Organización interna		
6.1.1 Compromiso de la dirección con la seguridad de la información	Aplicar	Requerimiento ISO 27001
6.1.2 Coordinación de la seguridad de la información	Aplicar	Requerimiento ISO 27001
6.1.3 Asignación de responsabilidades para la seguridad de la información	Aplicar	Requerimiento ISO 27001
6.1.4 Procesos de autorización para los servicios de procesamiento de información	Aplicar	La dirección debe de gestionar los nuevos recursos.
6.1.5 Acuerdos sobre confidencialidad	Aplicado	Requerimiento legal

Parte II. Implantación

- Crearemos los planes de tratamiento de riesgos.
- Se asignarán responsables y recursos.
- Detallaremos las tareas a realizar así como el coste de los planes.
- Crearemos el plan de trabajo para la implantación y justificaremos el coste total del proyecto.

Plan de tratamiento de riesgos

- Utilizando como referencia el documento de aplicabilidad se detallarán los planes de tratamiento de cada apartado del anexo que necesite implantar algún control.
- Se hará una estimación del tiempo necesario para la consecución de las tareas.
- Se detallará por cada plan las tareas y responsables encargados de llevarlas a cabo.
- Se justificará individualmente el apartado económico de cada tratamiento.

Plan de trabajo

- Con el plan de tratamiento de riesgos de todos los controles podremos crear el plan de trabajo del proyecto.
- El gasto total del proyecto quedará justificado.

Planes	Duración	Responsable
5 Plan de políticas de seguridad de la información	10 días	
Revisión de las políticas	5 días	Dirección y responsables de departamento
Creación de los procesos de difusión	5 días	Responsable de sistemas
6 Plan de la organización de la seguridad de la información	10 días	
Implantar sistema de mejora a través de gestor documental	4 días	Responsable de sistemas
Selección de personal para responsable de comunicaciones	5 días	Administración
Reuniones de la directiva con cuerpos de seguridad	1 día	Dirección
7 Plan de gestión de activos	10 días	
Instalar armarios seguros para documentación física	1 día	Responsables de departamento
Crear políticas de creación y migración de documentos al sistema ECM	6 días	Responsable de sistemas
Formación en gestor documental	3 días	Consultor externo
8 Plan de seguridad de los recursos humanos	10 días	
Formación	6 días	Consultor externo
Creación de proceso disciplinario	4 días	Administración, gerencia y consultoría legal

Parte III. Conclusiones y mejoras

- Existen muchas normas y certificaciones pero la ISO 27001 es una de las más importantes.
- La parte de análisis del proyecto es una de las más importantes y depende de la visión de quién implante la norma.
- Como resultado del proyecto el mayor gasto recae en la inversión de infraestructuras de la empresa.
- Como este trabajo abarca las dos primeras fases del ciclo de Deming convendría implantar las dos últimas que corresponden a la evaluación y eficacia de los controles (Check) y al mantenimiento y mejora del sistema (Act).

Gracias por su atención

Autor: Manuel Muñoz Martín

Tutor: Ana Cristina Domingo Troncho