Metodología de implantación y certificación en las PyMEs

PROCESO CONCEPTUAL Y OPERATIVO DE IMPLEMENTACIÓN DE ISO-27001

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

Este artículo presenta una primera parte, que es el desarrollo conceptual para llevar adelante la implementación de ISO-27001 en una PyME, y la segunda parte, presenta las fases y metodologías prácticas que implementa **NCS**, para preparación de PyMEs

1. Desarrollo conceptual.

El principal objetivo de este artículo es ofrecer un claro curso de acción para las PyMEs. No está orientado a las grandes empresas, pues cualquiera de ellas está en condiciones de contratar una consultoría externa y desentenderse del tema (…grave error), asumiendo también los grandes costes que ello implica. Por esta razón, es que toda PyME debe hacer una fuerte diferencia entre la **"Necesidad de certificar"** y el **"Negocio de la Certificación"**, que es la finalidad última de todo este texto pues, bien entendidas estas posturas es lo que les permitirá implementar a las PyMEs la mayoría de los puntos de este estándar, con gran independencia del "Negocio de la Certificación" que se gesta alrededor de todo estándar certificable.

Lo que se trata de reflejar en el cuadro anterior es la decisión que deberá adoptar todo responsable de sistemas en los próximos años, es decir:

Tal vez parezca cruel, o poco serio, pero es la cruda realidad *(a veces la realidad supera ampliamente a la ficción, y en este tipo de determinaciones puedo asegurarlo con mucha certeza)*.

> Es perfectamente posible preparar una PyME para luego solicitar la certificación ISO 27001

Se puede encarar esta ardua tarea, con la intención de aprovechar el esfuerzo o simplemente, para cumplir con un requisito que permita a la empresa seguir fielmente las exigencias del mercado y hacer el mínimo esfuerzo posible, tratando de (fría y crudamente) engañar al auditor…**(Lo que recuerden que, también afirmo y con mucha más contundencia, es que será imposible de mantener esta mentira)**. Puedo garantizar que será humanamente imposible volver a demostrar, año tras año, que el SGSI sigue rodando (la mentira tiene patas cortas). Es decir, no merece la pena tratar de encarar una futura certificación ISO 27001 si no se tiene como objetivo fundamental y sincero:

"Implementar un VERDADERO SGSI"

Esto se desmorona muy rápidamente si se partió de pilares débiles, engañosos o falsos, tratando meramente de obtener el sello de "ISO 27001" como única meta.

Por lo tanto, primer "consejo" (si se puede llamar así): **No se autoengañen, encaren esta tarea con la sana intención de aprovechar al máximo cada esfuerzo que esta les requiera**.

Una vez comprendido esto, creo necesario avanzar un poco más aún, pues esto afecta de lleno a las PyMEs y tal vez no tanto a una gran empresa.

Todo responsable de implementar ISO 27001 en una PyME, en mayor o menor medida, **"SÍ o SÍ" ¡¡ debe MOJARSE !!**

Evidentemente, necesito certificar ISO 27001 en el corto plazo:

Una gran empresa, tal vez pueda darse el lujo de externalizar todo el proceso, el mantenimiento y las acciones a futuro...una PyME seguro que no. A lo sumo, deberá contratar una consultora que le analice, diseñe, planifique e implemente inicialmente desde el vamos, todo el SGSI, pero es casi seguro que no podrá subcontratar el mantenimiento que un SGSI requiere, esta tarea implica poseer un claro entendimiento de lo que se hizo y el funcionamiento de todo el SGSI, por lo tanto, en cualquier caso alguien, responsable de la PyME deberá intervenir en profundidad. Esto no quiere decir que le implicará abandonar el resto de sus tareas, pero se debe ser consciente, que algo de su tiempo le deberá dedicar.

El responsable de seguridad de la PyME deberá "mojarse" desde el inicio. Puede hacerlo, embebiéndose del estándar, e ir preparando poco a poco su empresa con un mínimo apoyo de algún especialista. Este curso de acción, requiere un mayor esfuerzo de los administradores de informática de la empresa (y de su responsable), pero es el que mayor experiencia les aportará y, los resultados, si se ponen ganas, serán muy buenos y dejarán claros los pasos a futuro para mantener el SGSI funcionando perfectamente.

La segunda opción que puede tener el responsable de seguridad de una PyME, es contratar una consultoría para que lo guíe paso a paso en todo el proceso, ¡¡ ojo !!, no estoy diciendo que haga todo el trabajo, sino que vaya guiando a la empresa en cómo hacerlo, pues si lo hace la consultora, se cae en la mentira anteriormente mencionada, pues una vez que se retire el consultor, el SGSI será muy duro de mantener. Por lo tanto lo más importante a reflexionar sobre esta segunda opción es que no es "lavarse las manos", sino trabajar codo con codo con el consultor, para aprovechar al máximo la experiencia de éste en cada paso, y ser capaz de tener un claro conocimiento de todo lo

> Para serles sinceros, si se poseen los conocimientos y capacidades necesarias, afirmaría que se puede "dibujar" una certificación ISO 27001 (y lo que acabo de afirmar, es muy, pero muy atrevido...). Lo que también afirmo y con mucha más contundencia, es que será imposible de mantener esta mentira.

Establecer la relación entre la compañía y su entorno, identificando sus puntos fuertes y débiles

realizado, para mantenerlo en funcionamiento, se reitera que de esto se trata: "un ciclo de vida continuo".

En cualquiera de los dos casos, es perfectamente posible preparar una PyME para luego solicitar a los auditores acreditados la certificación ISO 27001.

2. ¿Cómo Propone NCS realizar esta tarea en una PyME?

Esta actividad de apoyo a las PyMEs que desean encarar un SGSI, independientemente que su objetivo sea certificarse o no (pues muchas lo lanzan únicamente para mejorar la gestión de su seguridad), desde NCS la hacemos de acuerdo a las siguientes fases:

- Análisis y Estudio del Ámbito de Aplicación (Alcance de la Certificación ISO/IEC 27001:2005).
- Identificación de Activos.
- Análisis de Riesgos (orientado a procesos de negocio).
- Declaración de Intenciones de la Dirección.
- Plan de Acción para implementar ISO/IEC 27001:2005.
- Inicio del Rodaje.
- Selección de Hitos (Medibles, demostrables: RODAJE).
- Estándar de Seguridad.
- Relación Documental.
- LOPD y LSSI (conformidades legales).
- Planeamiento y Ejecución de Formación y Concienciación.
- Auditoría Interna (plan, realización, resultados, mejoras).
- Preparación de Presentación del SGSI a auditores.

FASE 1: Análisis de la Situación Actual y Evaluación de la Seguridad

Objetivo: Identificar los objetivos de negocio, ya que el propósito de la certificación es garantizar la gestión de la seguridad sin perder de vista que esta ayuda al desarrollo de las actividades comerciales de la PyME.

Las **tareas** a desarrollar son:

1.– Se identifican cuáles son las principales actividades empresariales, reflejándolas en un diagrama de flujo.

2.– Se selecciona un alcance adecuado para el sistema, ya que el esfuerzo a la hora de implementar el SGSI debe ser proporcional al tamaño del sistema a construir.

3.– En base a la Norma ISO/IEC 27002:2005, se comprobará qué controles de dicha norma están implantados, y a qué nivel en base a un *checklist*. Con esto, se consigue determinar el estado de madurez en el que se encuentra la compañía, para poder identificar el esfuerzo que hay que hacer en la implementación.

FASE 2: Análisis y Gestión de Riesgos

Objetivo: Establecer la relación entre la compañía y su entorno, identificando sus puntos fuertes y sus puntos débiles, oportunidades y amenazas.

Las **tareas** a desarrollar son:

1.– Análisis de Riesgos.

2.– Tratamiento de Riesgos.

FASE 3: Lanzamiento del SGSI

Objetivo: Desarrollar los procedimientos necesarios que permitan implantar los controles seleccionados. En cada procedimiento se detallan los objetivos que se pretenden cubrir, cómo se implantan, y las responsabilidades asociadas.

Las **tareas** a desarrollar son:

Definición del SGSI:

a) Se define la Política de Seguridad que establece de forma clara el enfoque de la política de actuación de la compañía, el alcance y los objetivos globales.

b) Se recopilan los documentos relativos a la seguridad, existentes en la compañía.

c) Se elaboran y estructuran los procedimientos de gestión y funcionamiento del SGSI, que darán soporte a la Política de seguridad definida para la compañía.

d) Se desarrolla una bitácora de actividades en donde se van registrando los hitos alcanzados y las actividades que se están desarrollando a lo largo del tiempo.

FASE 4: Implantación y Puesta en Marcha del SGSI

Objetivo: Poner en marcha las políticas y procedimientos definidos en las fases previas, tomando previamente en consideración el necesario aprovisionamiento de fondos y la asignación de responsables.

Las **tareas** a desarrollar son:

1.– Formular e implementar un Plan de Tratamiento del Riesgo que identifique

las acciones, responsabilidades y prioridades de la Dirección para la gestión de los riesgos de la seguridad.

2.– **Implantar Planes de Formación y Concienciación:**

a) Impartir Planes de Formación sobre los nuevos procedimientos.

b) **Impartir Planes de Concienciación** sobre los beneficios que tiene implantar un SGSI en la compañía.

3.– Implantar el SGSI:

a) Implantar políticas y procedimientos del SGSI.

b) Implantar los controles seleccionados en el documento Declaración de Aplicabilidad.

> Hay que trabajar codo con codo con el consultor, para aprovechar al máximo la experiencia de éste en cada paso

FASE 5: Control y Revisión del SGSI

Objetivo: Realizar revisiones sobre la efectividad del SGSI atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de las auditorías de seguridad, incidentes, resultados de las métricas, y observaciones de las partes interesadas.

Las **tareas** a desarrollar son:

1.– Controlar el SGSI:

a) Se detectan los errores en los resultados del tratamiento de riesgos.

b) Se identifican y detectan las incidencias de Seguridad.

c) Se controla que las actividades de seguridad son realizadas correctamente, tanto por la tecnología implantada, como por las personas en las que se ha delegado la responsabilidad.

d) Determinar las acciones para resolver las brechas de seguridad de acuerdo a la prioridad de los negocios.

e) Se establecen métricas de seguridad para medir la eficacia y eficiencia del SGSI (ISO 27004).

f) Se determina las acciones llevadas a cabo para resolver una incidencia de seguridad son las adecuadas.

2.– Revisar el SGSI:

a) Realizar auditorías y revisiones por la Dirección del SGSI:

- Se revisa la Política de Seguridad y el Alcance del SGSI.
- Se revisa el Análisis de Riesgos.
- Se revisan los controles implantados.
- Se realizan auditorías internas y externas.

FASE 6: Mantenimiento y Mejora del SGSI

Objetivo: Implementar las mejoras identificadas a partir de los resultados obtenidos en las fases anteriores, asegurando que éstas permitan alcanzar los objetivos del SGSI.

1.– Mantenimiento del SGSI:

a) Se comunica a las partes interesadas las acciones y mejoras.

b) Se ejecutan las acciones correctivas y preventivas.

2.– Mejora del SGSI:

a) Se implantan las mejoras del SGSI que se han identificado.

Para serles sinceros, si se poseen los conocimientos y capacidades necesarias, afirmaría que se puede.