



LA NORMA **ISO 27001** Y SUS RETOS

Retos en la Seguridad de la Información

Fidel Maldonado

La seguridad de la Información comienza a ser un tema prioritario debido a las condiciones macro económicas y globalizadas que se viven hoy en día. La dependencia de servicios personalizados ha potencializado la necesidad de garantizar que la información disponible sea íntegra y confidencial, ya que cada vez se maneja un mayor volumen de datos sensibles.

A partir del 6 de Julio de 2010 entró en vigor la Ley Federal de Protección de Datos Personales en Posesión de Particulares (**LFPDPPP**), la cual obliga a que todos los particulares que obtengan, manejen o resguarden datos personales cubran las disposiciones de integralidad y confidencialidad.

Es por eso que las organizaciones se ven en la necesidad de implementar estándares que le ayuden a proteger tanto la información como sus activos, y es ahí en donde la norma Internacional **ISO/IEC 27001:2013** entra en función. Ésta gestiona la seguridad de la información a partir de una serie de requisitos enfocados a establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (**SGSI**).

Esta norma se encuentra dividida en dos partes. La primera se compone

de diez puntos entre los cuales se encuentran los siguientes:

- objetivo y campo de aplicación
- referencias normativas
- término y definiciones
- contexto de la organización
- liderazgo
- planificación
- soporte
- operación
- evaluación de desempeño
- mejora

La segunda parte, está conformada por el anexo **A**, el cual contiene los nueve Dominios y los 114 controles que forman la base del **SGSI**.

- **A.5** - Política de Seguridad de la información
- **A.6** - Organización de la seguridad de la información
- **A.7** - Seguridad ligada a los recursos humanos
- **A.8** - Gestión de Activos
- **A.9** - Control de Accesos
- **A.10** - Criptografía
- **A.11** - Seguridad física y ambiental
- **A.12** - Seguridad de las operaciones
- **A.13** - Seguridad en las comunicaciones
- **A.14** - Sistemas de información, adquisición, desarrollo y mantenimiento

- **A.15** - Relaciones con los proveedores
- **A.16** - Gestión de incidentes de la seguridad de la información
- **A.17** - Aspectos de la seguridad de la información en la gestión de la continuidad del negocio
- **A.18** - Cumplimiento

El propósito de este artículo es dar a conocer de manera general aquellos elementos que le apoyaran para llegar a buen puerto con la implementación de su **SGSI**, por medio de una serie de pasos sencillos que usted podrá implementar en su organización para no caer en las situaciones descritas.

De manera general los proyectos de implementación **SGSI** se desfasan debido al pobre entendimiento de las implicaciones en función de los requisitos de la norma **ISO/IEC 27001** por parte del negocio. Las **MIPYMES** son el sector más susceptible a sufrir desfases, debido a la necesidad de realizar inversiones que no están consideradas de manera inicial en el proyecto, pero que son necesarias para poder facilitar la gestión de los controles.



Antes de la implementación (Idealización y Estrategia)

Es necesario que antes de comenzar con la planeación y definición del **SGSI** se tomen el tiempo suficiente para llevar a cabo la identificación de sus capacidades organizacionales, considerando los recursos de los cuales se podrá echar mano para la implementación, así como el periodo por el que pasa la organización para comenzar la implementación, sobre todo si hay patrones de actividad del negocio que indiquen tendencias en la disponibilidad de los recursos.

La mayoría de las organizaciones cuentan con recursos capacitados en **TI**; sin embargo, la implementación de esta norma requiere de perfiles especializados en seguridad de información. A pesar de las claras diferencias, hay organizaciones en donde aún no se distinguen los alcances y responsabilidades de cada una de estas áreas, por lo tanto se recomienda revisar los perfiles de los recursos para garantizar que sean los correctos, especialmente en lo que concierne a las actividades del *Chief Information Security Officer* (**CISO**).

Si bien, es necesario que se haga una evaluación de los recursos, también será necesario identificar las capacidades técnicas de la organización a partir de la identificación de las herramientas y sistemas organizacionales que estarán involucrados dentro del **SGSI**. Es recomendable que a la par, se comience con

la identificación del software licenciado para garantizar que se cuente con los recursos necesarios.

Un tema vital a considerar, previo a la implementación, es la evaluación de la cultura organizacional, ya que esto nos ayudará a planear una estrategia de concientización e involucramiento de toda la organización. Por ello, es necesario identificar a las personas que participaran de manera directa en la implementación del **SGSI** (*stakeholders*), ya que serán quienes nos apoyarán en la comunicación de mensajes y en la implementación de los controles. Será igualmente necesario definir los roles en función del liderazgo.

El invertir tiempo en la identificación de estos cuatro elementos reducirá de manera significativa los riesgos de que se presenten desfases durante el proyecto. Tales como el que no exista el suficiente compromiso por parte de los involucrados o que el personal se sienta rebasado en sus capacidades, y que esto provoque el decaimiento del ánimo en la organización.

Durante la implementación (Planeación, Transición y Operación)

El éxito de la implementación del **SGSI** es la planeación. Comúnmente se orienta la implementación de este estándar a las áreas de **TI**, cuando en realidad se requiere de un equipo interdisciplinario que apoye a la consecución del objetivo, por lo que será recomendable considerar la inclusión de un administrador de

proyectos que apoye en la gestión de los temas del proyecto y lleve el control de tiempos, recursos y objetivos.

La administración de los riesgos deberá ser un tema recurrente con la dirección de la organización, ya que éstos se volverán prioritarios para garantizar no sólo la continuidad del proyecto, sino inclusive del negocio. Los riesgos deberán ser declarados de manera oportuna (en cuanto sean detectados) y se les deberá dar seguimiento hasta la mitigación de los mismos, por lo que será necesario contar con un plan de comunicación que considere los mecanismos, canales, mensajes y audiencias para cualquier tema relacionado con el proyecto.

Debido a la naturaleza de la norma, será necesario realizar un plan de inversión en donde se prioricen las capacidades del negocio y los tiempos de aprovisionamiento. Un error común es considerar sólo el tiempo de asignación del presupuesto, y se dejan fuera los tiempos que tarda el proceso de adquisición e implementación de las nuevas tecnologías.

Una vez que se ha terminado la planeación, el primer tema a tratar deberá de ser la concientización. Mientras más pronto se involucre al personal de la organización, es mejor. Las primeras sesiones deberán enfocarse a explicar cuál es la necesidad de la implementación de controles de seguridad, cómo podemos participar y entender cuál será



el plan de trabajo. Posteriormente deberá comunicarse la política de seguridad de la información, y solicitar apoyo para la identificación de riesgos desde las estaciones de trabajo.

Acto seguido, se comenzará con la identificación de los activos de la organización para realizar el análisis de riesgos, que es la base sobre la cual girará el [SGSI](#). Es importante mencionar que a la par de que se genera el análisis de riesgos, se puede realizar el control documental y de registros, acciones correctivas o preventivas, auditorías y de mejora continua, con el fin de dar paso a la documentación de los procesos de incidentes, requerimientos, problemas, cambios, liberaciones, capacidad, continuidad, disponibilidad, activos del servicio y configuraciones, así como proveedores.

Ahora sí estamos listos para implementar los controles que sean necesarios con base en el análisis de riesgos. No hay que olvidar generar el plan de tratamiento de los riesgos y el estatuto de aplicabilidad ([SOA](#) por sus siglas en inglés). Es recomendable elaborar un documento central del cual se desprendan los controles y lineamientos al cual normalmente llamamos manual de políticas.

Ya que tenemos lista toda nuestra documentación, estamos en posición de echar a andar todo nuestro [SGSI](#), aunque siempre será recomendable comenzar a implementar una

vez que se defina y documenten los controles, con la finalidad de tener un mayor tiempo de interacciones a fin de optimizar nuestros procesos.

Cuando el [SGSI](#) ya esté en operación, tendremos que conseguir evidencia de la aplicación de todo el proceso, previo a solicitar la auditoría de un organismo certificador. Éste, por lo general, dividirá la auditoría en dos fases:

- **FASE UNO.** La revisión documental que garantice la adecuada integración de los procesos y controles.
- **FASE DOS.** La revisión de los registros para garantizar que el [SGSI](#) opera con base en lo que se diseñó.

Después de la implementación

Una vez que se emite el dictamen de certificación, deberá realizarse al menos una auditoría de seguimiento cada doce meses, por un periodo de tres años, hasta que expire el certificado; en el tercer año deberá realizarse de nuevo la auditoría de certificación para poder mantenerla.

La actividad clave para garantizar la vigencia del certificado se centra en el monitoreo del cumplimiento del [SGSI](#), así como en el reforzamiento de la cultura de seguridad de la información dentro de la compañía. Es importante que el personal se tatúe la camiseta y sea consciente de que la seguridad es responsabilidad de todos.

Ahora, usted ya cuenta con una mejor idea de qué elementos debe

cuidar al momento de implementar un [SGSI](#). La mejor opción siempre será solicitar el apoyo y guía de una consultoría que tenga experiencia en implementación y certificación de estos procesos.

A finales de diciembre de 2013, al menos 22,293 certificados [ISO/IEC 27001:2005](#) (un crecimiento del 14%) fueron emitidos en 105 países y economías, dos más que en el año anterior.

Los tres principales países para el número total de certificados emitidos fueron Japón, India y el Reino Unido; mientras que Italia, la India y el Reino Unido fueron los tres primeros para el crecimiento en el número de certificados.