La familia ISO 27000 - 21/07/2007

El pasado primero de julio, ISO publicó "Technical Corrigendum", una corrección técnica para sustituir la numeración "17799" por "27002" en el documento, hasta esa fecha conocido como ISO/IEC 17799:2005.

El documento es sólo eso: una corrección en un documento de apenas una hoja, para hacer oficial el nombramiento.

La ISO ha reservado la serie ISO/IEC 27000 para una gama de normas de gestión de la seguridad de la información de manera similar a lo realizado con las normas de gestión de la calidad, la serie ISO 9000.

La numeración actual de las Normas de la serie ISO/IEC 27000 es la siguiente:

- **ISO/IEC 27000: Fundamentos y vocabulario.**
- **ISO/IEC 27001: Norma que especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI). Es la norma más importante de la familia.**
- **Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.**
- **ISO/IEC 27002: (previamente BS 7799 Parte 1 y la norma ISO/IEC 17799): Código de buenas prácticas para la gestión de Seguridad de la Información.**
- **ISO/IEC 27003: Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es el soporte de la norma ISO/IEC 27001.**
- **ISO/IEC 27004: Métricas para la gestión de Seguridad de la Información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.**
- **ISO/IEC 27005: Gestión de riesgos de la Seguridad de la Información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001.**
- **ISO/IEC 27006: Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la Seguridad de la Información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.**

¿Por qué hay que certificar la seguridad informática bajo la norma ISO 27001?

Al momento de explicar por qué certificar una norma internacional enfocada en la gestión de riesgos asociados a la seguridad de la información, como lo es la serie de normas ISO 27000 y en particular su capítulo certificable, es decir la norma ISO 27001, uno podría comenzar justificando su posición desde distintos ángulos.
Por ejemplo, analizando retornos de inversión en distintos escenarios de implementación, ventajas desde el punto de vista de costos, reconocimiento de la marca, aspectos regulatorios, relación entre la norma internacional y otras regulaciones locales, mostrar la sinergia entre distintos sistemas de gestión que probablemente ya se encuentren implementados o en camino de estarlo como ISO 9000, ISO 14000 o ISO 20000 entre otros.
Podríamos comenzar también por algo mucho más complejo: detallando cuáles son los riesgos que la norma ayudaría a mitigar, a partir de los cuales todos los demás aspectos se deducen de forma mucho más sencilla.

¿Pero por qué resultan tan difícil de describir los riesgos? Justamente porque no se quedan quietos, es decir, constantemente evolucionan.
Siempre están latentes, aunque no se dejan ver tan fácilmente.

De esta manera, si el día de hoy, como sugiere la norma, realizáramos una lista de activos, detalláramos todas las amenazas que los afectan, las vulnerabilidades asociadas a esas amenazas, y por último hiciéramos una valoración de los riesgos resultantes en función de su impacto y probabilidad de ocurrencia, podríamos asegurar que al otro día, esa valoración estaría desactualizada.

Y es por ese motivo que la norma comienza definiendo el sistema de gestión que servirá de base para administrar los riesgos, antes de comenzar a tocar siquiera cuestiones relacionadas a la seguridad: sistematizar el descubrimiento, tratamiento y mitigación de los riesgos, y sostener esas actividades en el tiempo, es condición necesaria para considerarse "mínimamente seguro", con todas las dificultades (y críticas justificadas) que expresarlo de esa manera podría acarrear.

Luego de haber implementado un sistema de gestión del riesgo, con todas las consideraciones mencionadas, incluyendo revisiones periódicas de un Comité de Seguridad que asigne recursos, verifique la implementación de los controles, propicie la mejora continua de los procesos, y ajuste políticas organizacionales que complementen las medidas de seguridad incorporándolas a un plan de capacitación y concientización para todos los actores que

interactúan con la información de la compañía, tendremos apenas un vistazo a lo que significa contar con ISO 27001 en una organización.
Esta norma se relaciona con todas las áreas y procesos de la empresa, incluyendo Recursos Humanos, Tecnología y Legales, produciendo también uno de los cambios culturales (y políticos) más importantes de los últimos 10 años en las organizaciones en general, que es la separación de funciones entre las áreas de Tecnología y Seguridad, que debe reportar idealmente en forma directa al CEO y/o al Directorio.

Pero el objetivo de la nota no es hablar solamente de ISO 27001, sino también de por qué conviene certificar la implementación de la norma: ¿es que solamente con implementarla no basta?

Desde mi experiencia, la certificación agrega un componente fundamental, que son las auditorías externas: éstas son realizadas (idealmente) por auditores profesionales que día a día van ganando experiencia en auditar organizaciones en distintos mercados, países y tipos de negocio, aportando objetividad al sistema de gestión implementado a través de las observaciones y no conformidades que detectan.
En un sistema de gestión ISO, es deseable que aparezcan aspectos a mejorar, ya que de otra forma para qué desearía uno contar con un sistema basado en la mejora contínua, y cuando solamente se realizan auditorías internas, estamos perdiendo una oportunidad inmejorable para validar la efectividad de las gestión de riesgos.

Ahora sí podemos volver al inicio de la nota y listar todas las ventajas que con seguridad contaremos luego de obtener la certificación, siendo conscientes que detrás de un certificado, hay muchos más beneficios para la organización aunque a veces: "lo esencial es invisible a los ojos.