Problemática, ventajas y desventajas de ISO-27001 en PyMEs

EL DISCURSO FINAL Y CONVINCENTE SE LOGRA CUANDO SE HAN SABIDO LLEGAR A IDENTIFICAR CLARAMENTE LOS "PROCESOS DE NEGOCIO", Y SOBRE ELLOS CENTRAR LA MÁXIMA ATENCIÓN DE SEGURIDAD

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

En estas líneas, continuando con los artículos sobre ISO-27001, trataremos de presentar el lado bueno y el "oscuro" de la norma. Pero para no perder la esperanza, lo haremos primero, dando a conocer la forma de resolver la problemática, para mantener la fe. Luego, incrementaremos la ilusión a través de las ventajas que ofrece. Y por último (casi en letras pequeñas) daremos un par de desventajas, para que no pensemos que es todo perfecto en esta vida.

Problemática

Tal vez la mayor problemática que posea una PyME para encarar ISO-27001, es lograr convencer a su Dirección de la importancia que reviste todo el proceso de implementación de la misma.

El discurso más eficiente parte, sin lugar a dudas, de los dos mayores argumentos que diferencian ISO-27001 de ISO-17799, pues el resto es lo que tienen en común, es decir los "controles" (que hoy ya se denominan ISO-27002). Estos controles, son sencillamente varios grupos de medidas técnicas, que como corresponde, no convencen a ningún director (pues, con mis mayores respetos, no saben de lo que le estamos hablando). Estos dos "nuevos" argumentos SÍ convencen a los cargos jerárquicos; son propios del lenguaje gerencial. Ya los hemos mencionado en otras oportunidades, y son:

> La mayor problemática en una PyME para encarar ISO-27001, es convencer a su Dirección de la importancia que reviste el proceso de su implementación

El análisis de Riesgo (AR)

La puesta en funcionamiento de un verdadero SGSI (Sistema de Gestión de la Seguridad de la Información) requiere los controles que a continuación avanzamos.

a. **El análisis de riesgo**

En la secuencia natural para obtener resultados del análisis de riesgo, es:

La identificación, definición, descripción y valoración de los activos.

El cálculo de impacto (debilidades, riesgo, grado de exposición, popularidad, criticidad, etc.) que podría ocasionar cualquier problema sobre cada uno de ellos.

El riesgo concreto que se posee de producirse determinados hechos.

Las salvaguardas que se pueden aplicar para minimizar el riesgo.

Conjunto de acciones que pueden realizarse (En lo posible agrupadas por similitud o área).

Propuesta de varios cursos de acción posibles (desde el de máxima, intermedios al de mínima).

Finalmente: Elección y Aprobación de un curso de acción por parte de la Dirección. Es decir, el compromiso que asume en virtud de su propia estrategia (Coste/Beneficio/Negocio), para tratar las acciones de ese curso de acción y ASUMIR el riesgo residual que quedará con lo que no esté dispuesto a abordar el máximo nivel de la empresa (o en definitiva a pagar…).

El último paso que trato es el más importante de todos, pues recién a partir de éste, se puede iniciar el conjunto de medidas para minimizar los riesgos, y a su vez para ir solucionando los impactos que SÍ esté dispuesta a abordar la Dirección ("por escrito": Declaración de intenciones). Lo cual dará como resultado un nuevo análisis de riesgo, para ver cómo evolucionaron las acciones, y los nuevos riesgos residuales… y las nuevas decisiones estratégicas… y las nuevas acciones… y las nuevas mejoras… y las nuevas… al fin y al cabo de esto se trata la idea de ciclo, gestión o PDCA.

El discurso final y convincente del AR se logra cuando se han sabido llegar a identificar claramente los "Procesos de negocio", y sobre ellos centrar la máxima atención de seguridad. Esto es lo que da de comer a la empresa, y todo Director necesita dormir tranquilo sobre ellos. Por lo tanto, si esto se ha hecho bien, tenemos grandes posibilidades de haber ganado esta "primer batalla", logrando que a través del curso de la acción que la Dirección haya elegido, podamos empezar nuestro trabajo.

b. **SGSI**

La segunda estrategia para obtener el éxito de nuestra problemática, pasa por el SGSI, el cual como su nombre indica, es un proceso de gestión, cosa que también conoce con alto grado de detalle un director.

Lo mejor que podemos hacer es respetar estrictamente lo que propone la norma como PDCA (Plan-Do-Check-Act), y asegurar que desde el primer día el sistema entrará en "rodaje". Esto implica que se pueden planificar seriamente sus acciones, hitos y evolución. Si se sabe presentar bien el SGSI, éste es otro logro, pues un sistema que "rueda", a través de los ciclos que va sufriendo, puede demostrar con máxima eficiencia su evolución la cual, en términos jerárquicos de la empresa, indica claramente, cómo se emplean los recursos que nos dieron. A través de cuadros de mando, pueden verificar cuantitativamente si se están empleando con corrección los mismos, cosa que en nuestro trabajo diario en seguridad, se nos suele hacer muy difícil de "poner en el escaparate directivo". Es decir, los planteos que ISO-27001 hace para implementar un SGSI, son discursos netamente convincentes.

Abandonar por un cierto tiempo el SGSI, requerirá un esfuerzo similar a lanzarlo de nuevo

Ventajas

Se debe tener en cuenta que la seguridad al 100% no existe. La norma establece una metodología y

una serie de medidas que al menos busca una mejora continua y que, sin lugar a dudas, aumentará el porcentaje actual de cualquier empresa. Esta mejora en la seguridad se ve reflejada en una serie de ventajas que se describen a continuación.

Competitividad (Para ser sinceros)

Si se trata de ser sinceros… éste es el primer factor que le interesa a cualquier empresa. Esta norma, como se mencionó varias veces, será en el mediano plazo europeo, tan importante como hoy lo es ISO 9000. Es decir, poco a poco las grandes empresas, los clientes y partners comenzarán a exigir esta certificación para abrir y compartir sus sistemas con cualquier PyME. Es natural y lógico que así sea, pues es el único modo que puede garantizar un equilibrio en las medidas de seguridad entre esas partes. Y para decirlo crudamente, quien no la tenga, se quedará fuera.

Ahorro económico (¿…?) (¿Será el segundo factor en importancia?)

Las medidas contra incendios: ¿Son un coste o una inversión? ¿Cuánto vale la pérdida de información?

Es muy difícil cuantificar este concepto, pero cualquier empresario que sea consciente del coste que poseen sus sistemas informáticos, sabe fehacientemente, que cualquier daño, caída, pérdida, robo, falsificación, suplantación, fallo, error, inconsistencia, virus, demora, saturación, escucha, intrusión, acceso erróneo, respuesta errónea, atentado, catástrofe… puede ser grave. Lo sabe, es más, le teme no sólo al daño concreto, sino a la pérdida potencial que esto implica: imagen, difusión, desconfianza, pérdida de negocios e inversiones, etc. La certificación reduce enormemente estas situaciones.

La implementación de la norma, implica una visión de detalle de los sistemas, lo cual hará que las inversiones en tecnología se ajusten a las prioridades que se han impuesto a través del AR, por lo tanto no habrá gastos innecesarios, inesperados, ni sobredimensionados. Se evitan muchos errores o se detectan a tiempo gracias a los controles adecuados; y si se producen, se cuenta con los planes de incidencias para dar respuesta efectiva y en el tiempo mínimo. Se evita fuga de información o dependencia con personas internas y externas.

Calidad a la seguridad

La implementación de un verdadero SGSI transforma la seguridad en una actividad de gestión. Este concepto por trivial que parezca es trascendente, pues deja de lado un conjunto de actividades técnicas más o menos organizadas, para

> Los planteos que ISO-27001 hace para implementar un SGSI, son discursos netamente convincentes

transformarse en un ciclo de vida metódico y controlado. Es lo que se mencionó al principio, pone "calidad a la seguridad", que en definitiva, "calidad" es lo que se busca y exige hoy en toda empresa seria.

Reduce riesgos

Partiendo del AR que impone la norma, hasta la implementación de los controles, el conjunto de acciones adoptadas reducirá al mínimo todo riesgo por robo, fraude, error humano (intencionado o no), mal uso de instalaciones y equipo a los cuales está expuesto el manejo de información.

Concienciación y compromiso

El estándar crea conciencia y compromiso de seguridad en todos los niveles de la empresa, no sólo al implantarla, sino que será permanente pues se trata de un ciclo.

Jamás debe olvidarse: La Alta Dirección, no tiene por qué tener la menor idea de los aspectos técnicos de la Seguridad Informática (es más, sería un error que le dedique tiempo a aprender estas cosas. hasta es mejor que juegue al golf y allí concrete grandes negocios.).
Lo que tiene clarísimo es la relación: Coste/Beneficio/Negocio con una visión global de la empresa.
Y ahí sí sabrá elegir cuál es el mejor curso de acción, que deberá adoptar para su negocio global (si se lo hemos sabido presentar debidamente...).
Por lo tanto el trabajo importante es saber resumir/concretar el trabajo, de muchas semanas o meses que conlleva esta tarea, entre tres a seis CURSOS DE ACCIÓN, y una vez adoptada la decisión directiva, encontrar todos los medios de llevar adelante esta determinación (y por supuesto, generar el correspondiente "feedback").

Cumplimiento de la legislación vigente

Todos los aspectos de conformidades legales de la norma deben responder a la legislación del país, y se verifica su adecuación y cumplimiento. Por lo tanto la certificación garantiza este hecho y a su vez seguramente crea un marco legal que protegerá a la empresa en muchos flancos que antes no tenía cubiertos.

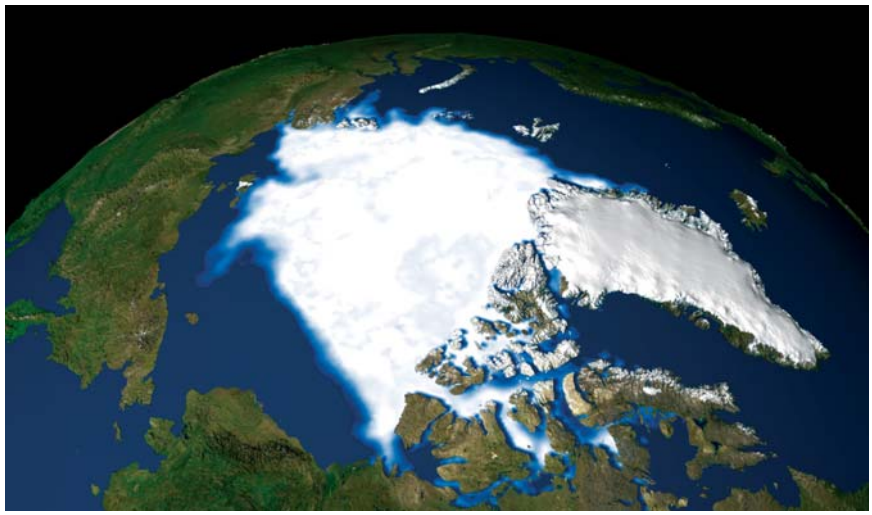
Visión externa y metódica del sistema

Todo el trabajo realizado para la implementación de la norma, implica una serie de medidas de auditoría interna que ofrecen ya de por sí un importante valor agregado; cada una de ellas responde a una secuencia metódica de controles. Un aspecto a considerar de este trabajo es la tensión y responsabilidad que impone al personal de la empresa, el hecho de estar pendientes de una futura certificación, como objetivo común. A su vez, llegado el momento de la certificación, los auditores, siguiendo los mismos pasos, darán una visión externa, independiente y totalmente ajena a la rutina de la empresa, que siempre aporta muchos elementos de juicio y acciones de mejora.

Supervivencia de mercado

Según un artículo publicado en *ComputerWeekly*, uno de los principales motores que están llevando al incremento de certificaciones ISO 27001 está siendo la aparición en contratos de sugerencias al proveedor respecto a estar certificado en esta norma.

Cada vez más contratos, al principio sólo gubernamentales pero también cada vez más en el sector privado, ya estipulan que el proveedor apropiado debería tener la certificación en ISO 27001 de Seguridad de la Información.



De hecho, algunas empresas que ya tienen la certificación ISO 27001 harán de *lobby* a favor de incluirlo como requisito en las ofertas de los clientes, obstaculizando a cualquier rival que no la tenga.

Por tanto y como nueva motivación, la certificación de la seguridad puede ser una oportunidad de negocio más que un coste.

Desventajas

Al iniciar este conjunto de tareas, no cabe duda que se está sobrecargando el ritmo habitual de trabajo de toda la organización, por lo tanto se debe ser conciente de que exigirá un esfuerzo adicional. Los que sufren estos incrementos son las personas, por lo tanto somos nosotros mismos los primeros en encontrarle y descubrirle las desventajas a ISO-27001, sobre todo antes de tomar la decisión de su lanzamiento, pues una vez encaminado.

No tiene retorno

Una vez que se ha empezado el camino de implementación de la norma ISO-27001, tenemos la opción de certificar o no. Sea cual fuere la elección, el cúmulo de actividades realizadas exige un mantenimiento y mejora continua, sino deja de ser un SGSI, y ello salta a la vista en el muy corto plazo. Es decir no se puede dejar de lado, pues al abandonar un cierto tiempo el SGSI, requerirá un esfuerzo similar a lanzarlo de nuevo.

Se debe tener en cuenta que la seguridad al 100% no existe

Si a su vez se obtiene la certificación, para que la misma se mantenga en vigencia, anualmente debe ser auditada por la empresa certificadora.

Requiere esfuerzo continuo

Independientemente de las tareas periódicas que implica una vez lanzado el SGSI para los administradores del mismo, el mantenimiento del nivel alcanzado, requerirá inexorablemente un esfuerzo continuado de toda la organización al completo.