ISO-27001 y las PyMEs

COMO EN TODO ESTÁNDAR, EL ÉXITO DE ISO-27001, ESTÁ SIENDO SU LLEGADA A LAS PYMES

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

Este artículo es el primero de una serie, que *serán todos orientados a las PyMEs*. En este, se va a tratar de "vislumbrar lo que se viene" para anticipar un poco lo que a las PyMEs casi les caerá impuesto. Esto no es una novedad, con ISO 9000 ya sucedió, la diferencia tal vez sea que este nuevo estándar está creciendo más vertiginosamente y a su vez toda PyME que desee seguir compitiendo en este "Cybermercado" necesitará cada vez más abrir/compartir sus SSII, deberá acceder y ser accedido a su información de stock, facturación, pedidos, clientes, productos, precios, listados, nómina, etc... y para ello le exigirán un cierto nivel de seguridad de los mismos. La mejor forma de demostrarlo es a través de una certificación reconocida mundialmente, y en esto, la calve la tiene ISO-27001.

Desde **NCS**, hemos querido vivir esta realidad en carne propia, para poder conocer en detalle todos sus aspectos, por eso empezamos a analizar este nuevo estándar desde hace casi dos años (acompañando a esta revista desde que nació, con las primeras publicaciones en ISO 27001) y en julio de este año obtuvimos la certificación. Nuestro ámbito a certificar fue el más amplio que se puede proponer una PyME: "***La totalidad de los Sistemas de Información***", este era el último eslabón que nos faltaba para poder ser verdaderos referentes en ISO-27001 orientado claramente dentro del marco de las PyMEs, conociendo el detalle de todo el proceso, su problemática, sus beneficios, ventajas y desventajas (de lo que hablaremos en otra ocasión). Hoy podemos decir que sabemos del tema, y en este artículo trataremos de reflejar nuestra experiencia.

> Si se asocian bien: procesos de negocio con activos fundamentales –> Seguridad: ya no es un gasto, sino un beneficio

Claves para una PyME

A nuestro juicio, existen cinco CLAVES para una PyME que se plantea ISO-27001 (cuestión que tal vez no sea así en una gran empresa):

- **Orientar la seguridad con sus procesos de negocio.**
- **Gestionar su seguridad** (no solo medidas técnicas).
- **Continuar su proceso de calidad.**
- **Obtener una validación sólida sobre su situación en LOPD y LSSI.**
- **Entrar en el proceso de "Lobby" que se está gestando.**

Desarrollemos brevemente cada uno de ellos:

a.) Orientar la seguridad con sus procesos de negocio:

El primer paso para la implementación de ISO-27001, es el análisis de riesgo (AR) (hasta podríamos discutir si es previo o no a la determinación del "Ámbito a certificar", pero no vale la pena hacerlo ahora....). Esta actividad, puede hacerse siguiendo cualquier metodología, siempre y cuando demuestre coherencia. El resultado final del mismo, será a través del análisis de activos, impacto, salvaguardas, etc, llegar a determinar los niveles de riesgo (fundamentalmente residuales) al que cada activo quedará expuesto, con la intención de "trabajar" de aquí en más sobre los mismos, en un ciclo continuo (Plan-Do-Check-Act). Hemos visto mucho de esto en la viña del Señor y estamos convencidos, que para una PyME lo fundamental, es que en el resultado final del mismo se vea claramente que lo principal para esta PyME es comenzar todo el trabajo por aquellos activos que "dan de comer

a la empresa", es decir los procesos primarios de negocio. Sinceramente, no nos sirve de mucho reconocer que la página web posee un alto riesgo, si esta empresa no opera a través de ella, es importante, pero no fundamental.

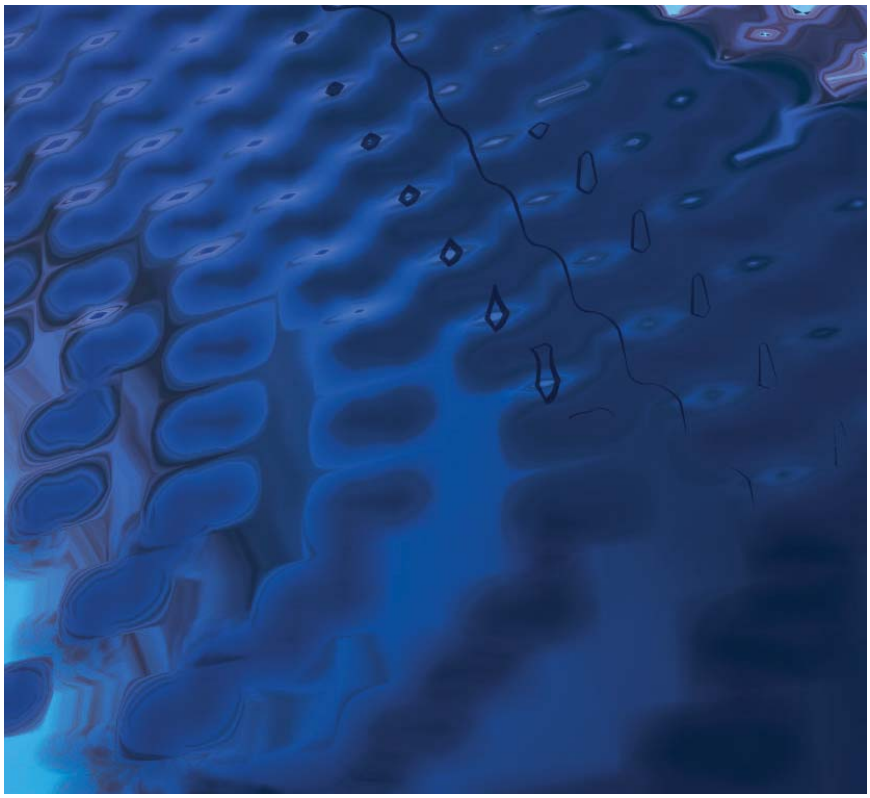
Si se han asociado eficientemente los procesos de Negocio con los activos fundamentales, entonces ahora se puede pensar la seguridad de los mismos como una cuestión ya no de gasto, sino de beneficio para esta PyME. Cada una de las acciones estará orientada a optimizar y garantizar el correcto funcionamiento de cada uno de ellos. Desde la contratación de personal, los acuerdos con terceros, la adquisición de hardware y software, la segmentación de redes, las medidas de seguridad física, hasta la preparación/prevención y tratamiento de incidentes, las conformidades legales, etc. Cada uno de estos temas estará centrado en su eficiente adecuación para el proceso de negocio.

Conclusión: el resultado final del AR, debe ser un *claro reflejo de lo prioritario* que es, para esta empresa en particular, *cada activo relacionado con sus procesos de negocio* (sino, ya empezamos mal...). Luego se optimizará cada uno de ellos.

b.) Gestionar su seguridad (no solo medidas técnicas):

El **holismo** enfatiza la importancia del todo, el cual, es más grande que la suma de las partes y da importancia a la interdependencia de estas.

Holismo, *eso es gestionar la seguridad*. Nuestra experiencia, es que la seguridad hasta ahora no dejaba de ser un conjunto de partes, conformadas por mayor o menor cantidad de medidas técnicas, según la empresa. ISO-27001, reúne la totalidad de ellas y al integrarlas a través de un Sistema de Gestión de la



Seguridad de la Información (SGSI) y llevado como un ciclo continuo (PDCA) genera holismo, un resultado superior a la suma de sus partes.

Esto no es una mera hipótesis, es el resultado que ofrecen los puntos 4 al 8 de ISO-27001. Hasta ISO-17799 (Actual ISO-27002), la seguridad era solamente una serie de 133 controles técnicos y nada más. La diferencia (Fundamental), entre su predecesora 17799 y la actual 27001, es que a través de esos nuevos apartados, **se genera un verdadero Sistema de Gestión** consensuado y llevado a la práctica mundialmente, pues se está demostrando que es la única forma de interpretar la seguridad, "como un todo" = **Holismo**.

> Se está demostrando que la única forma de interpretar la seguridad, es "como un todo": Holismo

Lo importante de esto para una PyME es que, es más grande que la suma de sus partes, y a través de estos puntos (4 al 8), *no deja nada librado al azar*, garantizando y homogeneizando el propio sistema con el de otras empresas, independientemente de la magnitud de las mismas.

c.) Continuar su proceso de calidad

Todo proceso tecnológico en Europa, se encuentra en una situación de necesidad de demostrar, garantizar y justificar su "Calidad".

Calidad, esa es la palabra clave de la Industria competitiva de este Continente.

Hoy en día, en casi todos los productos, el usuario final tiene una clara visión de lo que está comprando, y sabe casi con certeza, si se trata de un producto de buena, de dudosa, y/o de escasa calidad. Todo ello se debe a una serie de medidas, acciones, denominaciones, controles, garantías, certificaciones, y por supuesto la gran mayoría de ellos pasa por organismos reguladores, a los cuales ciertas industrias se esfuerzan por "escuchar y seguir" y otras no.

Al usuario final le llega esta imagen, gracias a toda una cadena industrial, que va desde la materia prima hasta el producto final. En el siglo XXI, uno de los pilares de esta cadena es la informática, por lo tanto si se está hablando de una cadena de eslabones compuestos por calidad, no queda más que volver al viejo dicho "*una cadena se corta por el eslabón más fino*".

Dentro de la Comunidad Europea, ya no se podrá admitir más que el eslabón más fino sea la informática, y cuando se habla de informática, la seguridad es uno de los pilares fundamentales que le da sustento, pues de nada sirve el mejor sistema, si este no está Disponible, No es Confiable, Su información es errónea o imprecisa,

> Hoy, la seguridad informática no puede ser el eslabón más fino en la cadena de calidad.

compromete a otras empresas o permite borrar hechos o transacciones, etc... De esto se trata ISO 27001.

Si tuviera que reducirse toda la norma en una frase sería:

ISO 27701
"Pone calidad a la seguridad"

Y, como se ha dicho hacia esto tiende toda la Unión Europea.

Esto no quiere decir, que el hecho de certificar una PyME en ISO 27001, garantice que esa empresa posee una "Excelente Calidad en sus niveles de seguridad", tampoco una persona por ser Ingeniero, Master o Doctor, garantiza que sea un excelente profesional, ***sólo puede garantizar que se ha realizado un serio y metódico esfuerzo por tratar de serlo***, y esto ya es un muy buen punto de partida.

d.) Obtener una validación sólida sobre su situación en LOPD y LSSI:

Para todas las PyMEs que tengan la incertidumbre de "Qué hacer con estos aspectos legales": Por fin llegó ISO-27001.....

Es interesante analizar este aspecto. Tanto en Europa como en EEUU, se están dando elementos de juicio que avalan este hecho.

A mediados del pasado mes de julio, se publicó en la revista "*Computer Weekly*" un artículo donde directivos de Microsoft, expresaban textualmente que ISO-27001, puede ser el puente de unión entre las orillas de la seguridad y las regulaciones legales. En el caso de este País, se refiere más a Sarbanes-Oxley e HIPAA. Pero en el caso concreto de España, ya hubo también algunos antecedentes concretos de inspecciones de la Agencia Protectora de Datos a empresas certificadas en ISO-27001 en los cuales, *al tomar conocimiento de la certificación, los responsables de esta agencia la consideraron como un trabajo superior aún* al solo hecho de la legalidad con la LOPD, pues evidentemente habían encarado un desafío mucho más grande, que incluía como parte de él, los aspectos relacionados con la protección de datos, y no hicieron ningún tipo de observaciones.

Estas consideraciones no pueden dejar dudas, pues el último grupo de controles de ISO-27001, se refiere a "Marco legal y buenas prácticas", y *su no cumplimiento es motivo de No Conformidad Mayor*, lo que ocasiona la no certificación. Es decir, el recibir la certificación ISO-27001, implica y avala, que los auditores correspondientes, han realizado una evaluación de las conformidades legales de la empresa y dieron el visto bueno... Se podría presentar una hipotética situación, en la cual una inspección de la Agencia de Protección de Datos o cualquier organismo oficial, ponga en duda lo controlado por la Autoridad Certificadora... humm... que incertidumbre... *¿Quién se animará a bombardear este puente primero?*

"ISO-27001, puede ser el puente de unión entre las orillas de la seguridad y las regulaciones legales"

e.) Entrar en el proceso de "Lobby" que se está gestando:

Uno de los principales motores que están incrementando las certificaciones ISO 27001 son la aparición en contratos, de sugerencias al proveedor respecto a estar certificado en esta norma.

La certificación de la seguridad puede ser una oportunidad de negocio más que un coste

Cada vez más contratos, estipulan que el proveedor apropiado debería tener la certificación en ISO-27001. Nuevamente no es de extrañarse, pues ya sucedió con otros estándares y es lógico que así suceda, pues estamos hablando de empresas que han decidido invertir en mejorar y garantizar sus SSII y otras que no.

Para no pecar de inocente, en este ámbito tan "sanamente" competitivo, es lógico pensar que algunas empresas que ya tienen la certificación ISO 27001 harán "lobby" a favor de incluirlo como requisito en las ofertas de los clientes, obstaculizando a cualquier rival que no la tenga (*no se porqué, me suena conocido este discurso...*).

Por tanto y como nueva motivación, *la certificación de la seguridad puede ser una oportunidad de negocio más que un coste*. Lo que no se puede pensar es obtener la certificación, por este sólo hecho, y muchísimo menos, hacerlo contra reloj pues sería inabordable.

En los próximos artículos trataremos los siguientes temas:

Problemática, ventajas y desventajas de ISO-27001 en PyMEs.

El nicho de mercado principal de ISO-27001 son las PyMEs.

Metodología de implantación y certificación en las PyMEs.