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

POR SU TAMAÑO, LAS PYMES TIENEN MAYOR FACILIDAD PARA CERTIFICAR SUS SISTEMAS DE INFORMACIÓN

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

Como la mayoría de los estándares, este también nace como una respuesta del mercado ante requerimientos concretos de seguridad. En definitiva, cualquiera de estas normas, lo que busca es homogeneizar las buenas prácticas que se comienzan a poner en marcha. Por eso todo proceso de estandarización de ISO, se inicia recolectando la opinión de las empresas del mercado que desean formar parte, proponiendo un primer borrador, y en base a las objeciones, comentarios técnicos, editoriales, etc. el borrador va madurando hasta llegar al nivel de estándar.

En este caso concreto, el tema venía fácil para las grandes empresas mientras fue ISO-17799. En definitiva solo era cuestión de implementar muchas medidas técnicas que se ajusten a los controles, pero al producirse el cambio a ISO 27001 (la parte certificable de la familia 27000) cuya diferencia de fondo no es trivial, podríamos afirmar categóricamente que el nicho de mercado de esta norma cambió radicalmente. La magnitud e implicaciones de un verdadero SGSI y un PDCA son tan considerables, que **una gran empresa lo tiene muy cuesta arriba** (y ya no tanto las PyMEs), y a los hechos me remito: No existe ninguna gran empresa que haya podido certificar el 100% de sus sistemas de información. Todas han empezado por acotar su ámbito de certificación, para avanzar paso a paso e ir creciendo hasta ver a dónde llegan. Es natural, pues desde la línea de partida es difícil ponerse de acuerdo, pues un análisis de riesgo que pretenda identificar TODOS los SSII que afectan sus procesos de negocio, para una gran empresa es imposible (insisto, me refiero a TODOS llegando al máximo nivel de detalle que permita concatenarse con la medición de impacto, las salvaguardas, y cuantificando el

> La familia ISO 9000, demostró con resultados concretos que la "calidad" fortalece el accionar de cualquier PyME

riesgo con valores concretos). Si no se puede partir de una base sólida, las inconsistencias se suman y se propagan, llegando a presentar serias brechas, para lo cual el mejor camino es "acotar la tarea", con un buen cimiento. Es decir un ámbito reducido, y luego seguir avanzando ladrillo a ladrillo. Esta metodología, aporta un "Know How" y una serie de documentos, procedimientos, medidas, acciones, concienciación, etc. que facilitará cualquier paso de ampliación a un futuro ámbito mayor.

Esta realidad de acotar el ámbito, podemos afirmarla pues justamente para corroborar este hecho, fue que en NCS nos propusimos la meta de certificar el 100% de nuestros sistemas y comprobar que esto es factible para una PyME, viviendo muy de cerca la dificultad que esto presenta a grandes empresas. Una PyME hoy, tiene el camino mucho más fácil, pues hasta la totalidad de su ámbito puede quedar bajo el control de un SGSI por la magnitud y sencillez que representa frente a una grande.

La familia ISO 9000, demostró con resultados concretos que la "calidad" fortalece el accionar de cualquier PyME, pues aumenta la eficacia, eficiencia, productividad, reducción de costes y mejora el funcionamiento de todos los procesos. Si se hace la analogía entre ambas normas, llegamos a la conclusión que su fondo es el mismo: Sistema de gestión de calidad, compromiso de la Dirección, gestión de recursos, medición, análisis, mejora continua. No puede ser de otra forma, las dos apuntan a la palabra mágica "Gestión". Todo responsable de una PyME, conoce mejor que nadie la diferencia entre "Administrar" y "Gestionar", la clave para este responsable, ahora pasa por volcar parte de su "expertiz" a la Gestión de la seguridad, y hasta tal vez descubra, cuando se involucre un poco, que sabe más que sus responsables de sistemas, pues ahora la PyME se dejará de "Administrar" (conjunto de medidas técnicas) la seguridad, para "Gestionar" (Ciclo: Planificar, actuar, medir, mejorar) seguridad, y en este terreno un conductor/organizador, se desenvolverá con mucha mayor soltura.

Si analizamos también la norma ISO 14000, nos pone en alerta sobre la tendencia hacia la calidad. Un hito, que se podría presentar casi como histórico fue el discurso de James Save, (Secretario del

Si no se puede partir de una base sólida, las inconsistencias se suman y se propagan

Comentario: al solicitar la certificación ISO-27001, se debe especificar un ámbito para la misma, este ámbito deja fuera todo lo que uno no desee cubrir por el certificado. Por ejemplo, se puede solicitar la certificación para el CPD central de la empresa, para el proceso de control de stock, de ventas, para la plataforma de transmisión de datos WAN, para la infraestructura informática de tal provincia, etc. Es decir, el certificado ISO-27001, solo aplica al ámbito en el cual se acotó la certificación, cosa que en el Logo que exhibe la empresa no figura, pero sí en el certificado (recomendamos especialmente, prestar atención a este hecho).

Departamento de Protección Ambiental ante el Senado de los Estados Unidos el 20 de marzo de 1996) donde expresaba "*que en la economía global actual las iniciativas de los gobiernos de los países industrializados están creando presiones de mercado tanto para las grandes compañías como para las pequeñas para que adopten las normas ISO 14.000, o dejarlas fuera de los mercados principales*". Es decir, la competitividad empresarial y gubernamental, exigen Calidad, exigen Gestión, y una vez más no me canso de recalcar "La seguridad no podrá ser más el eslabón más fino de esta cadena". La base productiva de un país son las PyMEs, por lo tanto el gobierno y las grandes industrias, se encontrarán tarde o temprano, con el compromiso de exigirla, al menos en un nivel homogéneo, y para ello el mejor aliado es ISO-27001.

En noviembre de 2005 (al mes de aparecer ISO-27001), Forrester publicó un informe en el cual ya destacaba que este estándar estaba empezando a ser empleado por empresas y administraciones públicas para validar la seguridad de socios de negocios previo al inicio de cualquier negociación.

> Una PYMEy, tiene el camino mucho más fácil hacia un SGSI que una grande

IRCA (International Register of Certificated Auditors) por su parte, en la publicación para la transición de auditores ISMS de ISO-17799 a ISO-27001, expresa textualmente "*Los SGSI se están transformando en un tema relevante a nivel mundial en un amplio rango de organizaciones y sectores industriales y comerciales*".

En definitiva, debemos remontarnos a la vieja idea de "**Calidad Total**", para la cual hoy ISO-27001 aporta una pieza más. Si rememoramos a sus pioneros, un muy buen consejo es el que figura en la Revista Harvard-Deusto Nº 59 de 1994 en el artículo "**Gestión de la calidad total en la pequeña empresa**" (Price, Michael J./Chen, Eva E.): "*La gestión de la calidad total (GCT) es también imprescindible en la pequeña empresa para conseguir* ***su viabilidad a largo plazo****. La GCT permite mejorar la calidad, incrementar la satisfacción del cliente y la competitividad de la propia empresa sin necesidad de sacrificar la innovación, la capacidad de respuesta rápida ni la aportación individual, que son claves de éxito*".

Como acabamos de expresar entonces, esta norma que propone "**Calidad en la gestión de la seguridad**", no está dirigida únicamente a grandes empresas, sino que casi lo contrario, deberá necesariamente ser aplicado en las PyMEs que deseen trabajar como socias de negocio de cualquier otra grande, pequeña empresa o en el ámbito de la administración pública. Todo indica que desde varios organismos oficiales se está apuntando a este hecho, a través de proyectos, subvenciones, gestiones, etc... Siempre tengo presente en mi vida un sabio refrán que dice "*La experiencia propia, cuesta mucho y llega tarde*", hoy la "Calidad y la Gestión", para cualquier PyME es una experiencia adquirida y asumida, creo que no hay que desaprovechar la oportunidad y simplemente, sumarle la palabra "seguridad" a este bagaje (sin que llegue tarde) para mantener su negocio "***...viable a largo plazo***".