La calidad en la seguridad: asignatura pendiente

PROBABLEMENTE, MUY POCAS EMPRESAS SON CONSCIENTES DE QUE LA CALIDAD EN LA SEGURIDAD NO ES ALGO NUEVO, SINO MÁS BIEN, UN HECHO TOTALMENTE REGULADO

Agustin Lerma
SECURITY MANAGER
NEXTEL, S.A

En 1999 se publicó la norma BS 7799 que consta de dos partes: **BS 7799-1 (ISO 17799-1**) Código de buenas practicas de seguridad de la información y **BS 7799-2** Implantación y certificación de un sistema de gestión de seguridad de la información. En el año 2002 se publica una revisión de la norma, cuya parte principal es la armonización entre controles y estructura de las normas BS7799, ISO 9000, e ISO 14000. Estas correspondencias se detallan en el Anexo C de la norma, y están enfocadas a obtener un sistema con estructura única de calidad y seguridad de la información.

El objetivo de la norma ISO 9001 es garantizar en las implantaciones de proyectos de seguridad unos niveles de calidad mínimos para obtener siempre la mejor protección. Por ello, la estructura documental y organizativa contempla los siguientes pasos:

- Definición previa del proceso de negocio de la empresa, que ayuda tanto a reducir el esfuerzo como la complejidad de la definición el alcance del SGSI además de la definición de los procesos de soporte del proceso principal de negocio.
- Una estructura documental, que proporciona la base del Registro principal de documentación (DML, o Document master list).
- Un procedimiento de clasificación y numeración de documentación establecido.
- Varios documentos ya en vigor compatibles con el esquema complementario de seguridad.
- Una cultura de empresa en cuanto a la difusión del conocimiento y a la formación de las persona y las herramientas de difusión, intercambio y registro de conocimiento y formación

> Muchas empresas solo desarrollan relaciones comerciales con entidades de su mismo estatus de calidad

Más allá de estos procesos, encontramos la norma BS 7799-2:2002, que aunque presenta importantes similitudes con la ISO 9001, también tiene algunas diferencias clave como la existencia de un procedimiento de castigo en caso de incumplimiento en el estándar de seguridad y la existencia de un elemento como un Plan de continuidad de negocio para la seguridad de la información. No debemos olvidad nunca que el **objetivo fundamental de un SGSI es proteger nuestro negocio y proporcionar continuidad a este en una situación de riesgo.**

Pero las similitudes son mayores que las diferencias. En los dos ámbitos, son las personas las encargadas de hacer que todo funcione correctamente. La información, formación y difusión de conocimiento sobre un esquema de calidad y un SGSI para los integrantes de una empresa es la tarea más importante y necesaria para que este sistema funcione.

Ambas normas se basan en una metodología de PDCA (Plan/Do/Check/Act), que permite poner un marcha un proceso de mejora continua. Así que en la estructura básica de operación utilizan la misma guía. Otro aspecto importante, es el compromiso de la Dirección de la empresa con la implantación de ambos esquemas. La certificación de una organización en ambos estándares por una Entidad de Certificación, supone entrar en un club donde sus miembros se reconocen como iguales.

Muchas empresas solo desarrollan relaciones comerciales con entidades de su mismo estatus de calidad. Esta situación se repetirá con el estándar de seguridad. Solo aquellas empresas que puedan garantizar que la información propia, de sus socios o de sus clientes, esta debidamente protegida podrán tener acceso a contratos que impliquen confidencialidad, integridad y disponibilidad de información. Ámbitos críticos serán la sanidad, banca, seguros, ingeniería, consultoria, telecomunicaciones, etc. Disponer de un SGSI es un elemento clave para la obtención del estatus necesario para obtener este reconocimiento, por lo que la seguridad de la información y la excelencia en calidad tienen un encaje probado y reconocido.

> La información, formación y difusión de conocimiento sobre un esquema de calidad y un SGSI para los integrantes de una empresa es la tarea más importante y necesaria

Por último, señalar que la metodología ITIL (Basada en BS 15000), de gestión de tecnologías IT, reconoce como válido un SGSI basado en BS 7799-2:2002 para la seguridad de la información. Sólo las empresas mas avanzadas a nivel europeo están trabajando con esta metodología. El objetivo es identificar las necesidades de empresas y personas, y utilizar SLAs (Service Level Agreements / Contratos de prestación de servicio) para asegurarse de que los recursos se dirigen a satisfacer esas necesidades y no otras. Este procedimiento eliminará la posibilidad de desperdiciar recursos en servicios no necesarios o no necesitados por los clientes, y ayuda a proporcionar los servicios realmente prioritarios y necesarios para los clientes.

Éste es el camino para obtener una estructura única de excelencia, basada en la mejora continua, y que proporcione mayores opciones de liderazgo de negocio.