La Calidad y la Gestión de la Seguridad de la Información.

Dentro del mercado internacional de certificación de Sistemas de Calidad normativos podemos encontrar un amplio espectro de normativas aplicables a casi todas las actividades existentes, normas de alcance no restringido al rubro, sector o prestación, otras aplicables a las especificaciones o variables de producto, las cuales sirven para normalizar la oferta de determinados bienes, e incluso a otras que tienden a regular actividades sensibles para las empresas o su mercado. Desde la década del '80 los esquemas de gestión normativos vienen avanzando a paso firme y continuo, y ganando en masividad y aceptación de la mano del estándar más reconocido de todos: ISO 9000. A medida que iba ganando en aceptación, el esquema ISO, por demás eficiente como herramienta de gestión integral del negocio (esto a partir del 2000), fue migrando, integrándose y conformándose en la base operativa de muchas otras normativas más específica para ciertos sectores o actividades, y de esa forma nacieron las normas aplicables al sector automotriz, por ejemplo. Otro caso es la practicidad ganada con los sistemas de calidad alimenticia, que lograron un alto nivel de eficiencia integrando las Buenas Prácticas de Manufactura o el HACCP a un esquema documental ISO 9001.

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es justamente eso: la evolución de la norma ISO 9001 y sus integrables, en un nuevo esquema de resguardo de documentación e información crítica en ciertos negocios. La creación del estándar que fija las pautas de construcción de un SGSI (o ISMS, por sus siglas en inglés), la norma ISO 27001:2005 puede encontrar su origen en dos hitos particulares: por un lado, la penetración de ISO 9001 a la actividad bancaria, al desarrollo de software y a la prestación de servicios de IT; y por otro lado al creciente nivel de regulación de entidades financieras, a fin de reducir el riesgo operativo.

Los que nos dedicamos a la implementación de Sistemas de Calidad normativos podemos reconocer en este nuevo estándar una mezcla de IT y metodología de aplicación de normas como la ISO 14001 o la OHSAS 18001. Se trata de asegurar la “estanqueidad” de los contenedores de información y datos críticos dentro de un sistema informático, y por otro lado la gestión de un sistema que permita tener bajo control y minimizar los riesgos de pérdida, destrucción, corrupción, filtración y visualización indebida de esa información o datos, por los cuales la empresa es responsable ante sus clientes, la entidad de control o el Gobierno. Supongamos que dejamos nuestros datos de tarjeta de crédito en poder de una firma comercial, la cual nos los solicitó para cerrar una transacción comercial; en ese caso la empresa es responsable legalmente por el destino de los datos que le entregaron, y la protección de los mismos, por lo tanto, debe ser tomada como una Política Organizacional.

La Calidad y la Gestión de la Seguridad de la Información.

Cuanto más crítica sea la información o documentación que un ente, organización o empresa maneje, más necesario se torna protegerla, guardarla y asegurar su incorruptibilidad, eliminar accesos irrestrictos a ella o evitar su pérdida o difusión, por cualquier medio. De eso se trata un SGSI y aquellos que trabajan con paquetes de datos de propiedad de terceros saben que tan sensible puede ser no atender al requerimiento de seguridad; la ley de Habeas Data (Ley de Protección de Datos Personales nro. 25326) se ocupa de ello. O quizá aquellos que manipulen información financiera puedan decir que ocurriría si dicho activo se perdiera, corrompiera o filtrara, afectando la confidencialidad y sustentabilidad del negocio; el Comité de Supervisión Bancaria de Basilea mediante el documento “Basilea II” y la réplica argentina a cargo del BCRA, la resolución A 4609, tienden a evitarlo.

Ya no podemos hablar la “nueva tendencia” hacia la informatización total de la economía, llegando al final del primer decenio del siglo XXI. De lo que sí podemos hablar es que ante la proliferación ilimitada de las tecnologías informáticas y sus aplicaciones a la vida diaria, es cada vez mayor la cantidad y calidad de información que corre por el interior de un sistema, el cual hace rato dejó de ser cerrado. Para ese sistema que hoy en día es evidentemente permeable, la construcción de Sistemas de Gestión de Seguridad de la Información es una necesidad imperativa.