

Excelencia Empresarial y Gestión de la Seguridad de la Información: Revisiones Legales en la ISO 17799

Hablar de *Excelencia Empresarial*, de forma genérica, es hacer referencia a medios, procedimientos, técnicas y prácticas profesionales en la gestión de una organización que permitan a la misma alcanzar una cota de mayor calidad y nivel de perfección; mejorar la gestión y los resultados. Toda organización que se precie necesita establecer sistemas de gestión apropiados para avanzar en el camino de la excelencia.

En pleno desarrollo de la Sociedad de la Información, uno de los sistemas a implantar es el relativo a la gestión de la información, convirtiéndose la misma en uno de los activos que toda estructura empresarial debe proteger y salvaguardar frente a un entorno adverso y un abanico de amenazas contra los principios básicos de la seguridad de la misma: confidencialidad, integridad y disponibilidad. Gestionar adecuadamente la seguridad de la información debe ser un medio encaminado a minimizar dichas amenazas, al tiempo que maximizar el retorno de la inversión y mejorar las oportunidades de negocio.

Ante estas circunstancias es imprescindible que toda organización, pública o privada, evalúe e identifique los riesgos asociados, estableciendo las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

En este sentido, fue aprobada la Norma ISO 17799, cuya adaptación española se denomina UNE-ISO/IEC 17799. Esta norma establece diez ámbitos o dominios de control, que cubren los aspectos más relevantes de todo proceso de gestión de seguridad de la información, si bien ello no impide que el número de controles pueda ser superior o inferior; los controles a efectuar dependerán de la propia organización y los objetivos que se pretendan alcanzar.

De los controles detallados en la UNE-ISO/IEC 17799 cabe destacar el relativo a la revisión de los aspectos legales y contractuales que sean de aplicación y relevancia a cada sistema de información. El objetivo de esta revisión legal es doble:

- Evitar los incumplimientos de cualquier norma, reglamento, regulación u obligación contractual que sea de aplicación.
- Diseñar, operar, usar y gestionar los Sistemas de Gestión de la Información de conformidad con las exigencias legales, reglamentarias y contractuales que sean de aplicación.

En este sentido, es recomendable recabar el asesoramiento jurídico de entidades que, como LEGALIA ABOGADOS, dispongan de especialistas en las diferentes áreas o materias legales implicadas para, de forma integral, centralizada y personalizada, puedan ayudar a resolver las concretas necesidades con todas las garantías exigibles.

El primer aspecto del control legal y contractual a tomar en consideración es llevar a cabo la identificación de la legislación aplicable al sistema de gestión de seguridad de la información que vaya a ser objeto de control. A su vez hay que distinguir entre:

- Aspectos jurídicos específicos del tipo de actividad en que se encuadra cada organización. Por ejemplo, sector sanitario, bancario, telecomunicaciones o seguros.
- Aspectos jurídicos comunes a todo tipo de organización.

El segundo aspecto del control legal a tomar en consideración es la revisión del cumplimiento de la legislación identificada, sobre la base de unos criterios previamente definidos, en función del alcance que se pretenda dar a la revisión de los aspectos legales y contractuales. Es decir, un "traje a medida" garantizando siempre unos mínimos.

En particular, de los aspectos jurídicos comunes a todo tipo de organización, la UNE-ISO/IEC 17799 identifica, de modo meramente enunciativo, los siguientes:

- Propiedad Intelectual.
- Protección de Datos de carácter personal.
- Uso de las herramientas tecnológicas por parte de los usuarios de los sistemas de información de la organización.
- Registros de información de la organización.
- Medios y procedimientos de preconstitución de medios de prueba.
- Reglamentación de los controles de cifrado y uso de firma electrónica.

Ahora bien, un rasgo que caracteriza a la UNE-ISO/IEC 17799 es el hecho de que la misma no es certificable; es decir, no nace con la voluntad de ser imperativa ni vinculante, sino más bien como una "guía práctica" donde se detallan unos controles y pautas que puedan ser observadas de forma voluntaria.

Relacionado con lo anterior, AENOR aprobó y publicó en febrero de 2004 la Norma UNE 71502, que lleva por título *Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)* y cuyo objeto es especificar los requisitos para establecer, implantar, documentar y evaluar un SGSI de acuerdo con la Norma UNE-ISO/IEC 17799. Un rasgo propio de la UNE 71502 es el hecho de ser certificable.

Analizando la relación entre las normas anteriormente indicadas, cabe señalar que si bien la UNE-ISO/IEC 17799 es una norma NO CERTIFICABLE, sin embargo recoge la relación de controles que se deberán evaluar para establecer un SGSI según la Norma UNE 71502, que sí es CERTIFICABLE. De este modo nos encontramos con que la Norma UNE 71502 es una norma carente de contenido sustantivo en la que únicamente se define el proceso que habrá de seguirse para implantar, documentar y evaluar un SGSI, remitiéndose, en cuanto a los controles que deberán implantarse, a los recogidos en la UNE-ISO/IEC 17799, entre otros, los legales y contractuales.

Por lo tanto, la certificación de un Sistema de Gestión de Información de conformidad con Norma UNE 71502, llevada a cabo sobre la base de los controles y estándares de la Norma UNE-ISO/IEC 17799, es una forma de contribuir a reducir, en la medida de lo posible, los riesgos de los sistemas de información de las organizaciones a través de una gestión eficaz de los procesos de seguridad y, consecuentemente, una forma de avanzar en el camino de la excelencia empresarial. Y un buen SGSI exige, ante todo, gestionar. Esto es, administrar, redactar políticas, normas y procedimientos, implantarlos y verificar su cumplimiento, siendo un proceso continuo que debe ser controlado, gestionado y monitorizado.

Juan Carrasco Linares

Responsable Dpto. Tecnologías de la Información – Oficina de Valladolid

© 2005 LEGALIA ABOGADOS

juancarrasco@legalia.com