Preámbulo

La reciente publicación de la Ley 8/2011, de 28 de abril y del Reglamento que la desarrolla mediante Real Decreto 704/2011, de 20 de mayo han venido a regular un aspecto, tan esencial para nuestra seguridad, como es la **Protección de las Infraestructuras Críticas**.

Dada la relevancia de esta regulación y el impacto que tiene sobre todos nosotros y, en especial, sobre el sector de la seguridad de las tecnologías de la información y las comunicaciones (en adelante, TIC) y los profesionales que a ella nos dedicamos, los tres capítulos de ISACA en España (Barcelona, Madrid y Valencia) hemos aunado esfuerzos para elaborar este documento de opinión sobre dicha normativa.

Uno de los objetivos en los que las tres asociaciones coincidimos es la búsqueda de la excelencia en la gestión TIC gracias al desarrollo y capacitación de los profesionales que a ella se dedican. En este sentido, existen algunos aspectos de la citada normativa sobre los que nos gustaría manifestarnos y expresar nuestra opinión al respecto. En concreto, nos referimos a los siguientes:

- Concreción de medidas y auditorías proactivas en los Planes de Seguridad del Operador y los Planes de Protección Específicos.
- Capacitación del Responsable de Seguridad y Enlace.
- Mecanismos de *enforcement*.

Planes del operador

En primer lugar, en relación a los **Planes de Seguridad del Operador y los Planes de Protección Específicos** que deben elaborar aquellas organizaciones que sean designadas como operadores críticos, echamos en falta un aspecto que consideramos básico para poder abordar cualquier proceso de cumplimiento: las medidas de seguridad mínimas, o al menos, los criterios de valoración.

Si el objetivo es "*garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales*", como indica el propio preámbulo de la Ley, consideramos un aspecto esencial que se definan cuales son las medidas de seguridad que se han de establecer, como mínimo, para proteger las infraestructuras críticas o al menos que se hagan públicos los criterios de valoración de los planes. En ambos casos, existe una consecuencia positiva clara, se elimina la incertidumbre del proceso de valoración y contribuye al establecimiento de un nivel mínimo de protección en todas nuestras infraestructuras críticas minimizando el efecto del *eslabón más débil* en el conjunto de las mismas, haciendo independiente el nivel mínimo de protección de las capacidades de negociación concretas de cada operador.

En especial, consideramos de especial importancia que se pudieran incluir en la legislación o en sus documentos de desarrollo, los procedimientos de actuación en caso de incidentes o los mecanismos que se emplearán para el intercambio de información entre los distintos agentes implicados (como, por ejemplo, con los agentes de Protección Civil).

Por otra parte, al margen de la exigencia de un proceso de revisión bienal de los Planes exigibles al operador, consideramos que sería un aspecto muy favorable que dicho operador pudiera presentar, de manera proactiva, el resultado de haberse sometido a una auditoría de conformidad con la Ley y todos sus desarrollos posteriores. Esta auditoría, cómo es lógico, debería haber sido realizada por profesionales cualificados. En este punto, quisiéramos destacar la valía de una de las certificaciones profesionales de ISACA, que acredita a los profesionales como auditores de sistemas de información, la certificación CISA (Certified Information Systems Auditor).

Responsable de Seguridad y Enlace

En segundo lugar, relativo al **Responsable de Seguridad y Enlace**, el hecho de que deba contar con la habilitación de Director de Seguridad expedida por el Ministerio del Interior supone, a nuestro juicio, un enfoque excesivo en lo que se ha venido denominando tradicionalmente como *seguridad física*, ya que es un título enfocado en la seguridad privada cuando, en la actualidad, uno de los componentes principales, si no el principal, es el riesgo tecnológico (como han puesto de manifiesto sucesos como el de Stuxnet).

Por lo tanto, consideramos esencial que para garantizar una adecuada protección de las infraestructuras críticas, se solicite un perfil más multidisciplinar y que se valoren otras capacitaciones profesionales que suponen el conocimiento y la experiencia en el ámbito tecnológico como es el caso de las certificaciones CISA (*Certified Information Systems Auditor*), CISM (*Certified Information Security Manager*) o incluso, la reciente CRISC (*Certified in Risk and Information Systems Control*).

Esta situación no es extraña puesto que actualmente ya existen otros organismos que requieren de dichas certificaciones para la realización de ciertos tipos de trabajos relacionados con los riesgos tecnológicos. Nos referimos, por ejemplo, al Estado de California, la Generalitat de Catalunya, la Sindicatura de Cuentas de Valencia o la Autoridad Valenciana Portuaria.

Mecanismos de *enforcement*

Por último, hay un aspecto que debería también clarificarse para conocimiento del sector y que va aparejado a cualquier normativa, nos estamos refiriendo a los **mecanismos que se utilizarán para garantizar que se aplica la legislación**. La naturaleza y la rigurosidad de dichas medidas serán un indicador de la seriedad con la que todos los actores considerarán esta nueva normativa.

Para finalizar, las tres asociaciones nos ponemos a disposición del **Centro Nacional para la Protección de las Infraestructuras Críticas – CNPIC** para colaborar, como entidades sin ánimo de lucro, en todo aquello que estuviera a nuestro alcance en línea con nuestros objetivos de buscar la excelencia en la gestión TIC sobre la base de la capacitación profesional. En este sentido, consideramos que podríamos ser de ayuda en aspectos tales como la formación de profesionales en lo relativo a la gestión de riesgos TIC, a la realización de estudios sectoriales, etc.

Madrid, a 15 de septiembre de 2011

Sobre ISACA:

ISACA cuenta en España con tres capítulos localizados en Barcelona, Madrid y Valencia con 1.600 asociados lo que les convierte en el grupo de profesionales más representativo en esta materia. Cada capítulo funciona como una asociación independiente realizando actividades de difusión, concienciación y formación propias, pero colaborando estrechamente siempre que es posible. Todos ellos realizan Congresos anuales, boletines para sus asociados y cursos de formación para contribuir a la misión de ISACA.

Con 95.000 miembros en 160 países, ISACA (www.isaca.org) es un líder global que provee de conocimiento, certificaciones, comunidades, apoyo y educación en materia de seguridad en sistemas de información (SI), gobierno corporativo y gestión de TI, riesgos relacionados con TI y cumplimiento normativo. Fundada en 1969, ISACA es una asociación independiente, sin ánimo de lucro que organiza conferencias internacionales, publica el ISACA® Journal y desarrolla estándares internacionales sobre auditoría y control de SI que ayudan a sus miembros a asegurar la confianza en, y el valor de los sistemas de información. Asimismo, avanza y da fe de las habilidades y conocimientos en TI mediante las certificaciones respetadas internacionalmente Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) y Certified in Risk and Information Systems Control™ (CRISC™). ISACA actualiza continuamente COBIT®, que ayuda a los profesionales de TI y a los líderes de las organizaciones a cumplir con sus responsabilidades en gobierno y gestión de TI, particularmente en las áreas de auditoría, seguridad, riesgo y control, así como proporcionar valor al negocio.