

Las Certificaciones de Seguridad en el ámbito del ENS

Hay un punto del Esquema Nacional de Seguridad (RD 3/2010) sobre el que no se entra en mucho detalle generalmente pero que puede tener su dosis de polémica en un futuro no muy lejano.

Se trata de las certificaciones en materia de seguridad recogidas en el artículo 18.

“Artículo 18. Adquisición de productos de seguridad.

*1. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por las Administraciones públicas se valorarán **positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.***

*2. La certificación indicada en el apartado anterior deberá estar de acuerdo con las **normas y estándares de mayor reconocimiento internacional**, en el ámbito de la seguridad funcional.*

*3. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información (CESTI), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, **determinará el criterio a cumplir en función del uso previsto del producto a que se refiera**, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.”*

De lo anteriormente expuesto se deduce que el CESTI va a jugar un papel fundamental para determinar qué productos son más válidos que otros en la implantación de infraestructuras bajo el ENS. Dicho de otra forma, quien tenga un producto homologado, estará en mejores condiciones que la competencia para vender a la Administración.

Qué es el CESTI.

Fue constituido por el Centro Criptológico Nacional (CCN) adscrito al Centro Nacional de Inteligencia (CNI) y es un laboratorio acreditado dentro del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información para:

- Evaluaciones ITSEC (Niveles: E1 - E4):
 - ITSEC son las siglas de “criterios de evaluación de la seguridad de la tecnología de la información” que fue publicado en 1990 y realizado por expertos de Francia, Países Bajos, Alemania y Reino Unido.

Posteriormente en 1991, la Comisión de las Comunidades Europeas publicó una versión mejorada para el uso operacional dentro de los esquemas de evaluación y certificación.

Los niveles E1-E4 abarcan distintos aspectos en el ciclo de vida de diseño de sistemas, desde arquitecturas a elección de lenguajes de programación, documentación del sistema etc. ITSEC fue siendo sustituido por Common Criteria.

- Evaluaciones ISO/IEC 15408 o CC (Niveles EAL1 - EAL4): Los “criterios comunes” son un marco de reconocimiento internacional para que los usuarios especifiquen sus necesidades de seguridad, los vendedores diseñen las características de sus productos, y los laboratorios puedan evaluar los productos para comprobar que satisfacen las demandas de los usuarios.

Ambas acreditaciones las concede ENAC y el CCN.

Conclusión, el CESTI sigue estándares internacionales de reconocido prestigio para certificar productos que serán objeto de uso dentro de proyectos bajo el Esquema Nacional de Seguridad.

Qué hace el CESTI.

- Acreditar a laboratorios para que estos evalúen la seguridad de productos de tecnologías de la información.
- Certificar productos por parte del CCN, que presenten los fabricantes: por ejemplo: aparatos de cifra, tarjetas PKI, etc... el CCN los examina los somete a un conjunto de pruebas y otorga su valoración sobre el grado de seguridad de los mismos.

¿Y los servicios?.

Es evidente que el proceso de homologación de productos se hace con rigor y de forma estricta, pero ¿no se hace ningún proceso de homologación de la capacidad de los prestadores de servicios?.

No basta con que una marca/modelo de equipo haga lo que dice hacer y además sea homologado. Cualquier equipo requiere de una instalación inicial, configuración, transferencia de conocimiento al cliente (administración es este caso), mantenimiento, actualizaciones de parches, documentación técnica etc. Es decir, cualquier equipo o dispositivo de seguridad, requiere necesariamente de una empresa por detrás que lo suministra, lo soporta y lo actualiza.

El ENS no habla absolutamente nada sobre la cualificación de empresas y sobre certificaciones exigibles, pero la ley 30/2007 de Contratos con el Sector Público si o

hace.

“Artículo 10. Contrato de servicios.

Son contratos de servicios aquéllos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o un suministro. A efectos de aplicación de esta Ley, los contratos de servicios se dividen en las categorías enumeradas en el Anexo II.”

En este Anexo se comprueba que quedan incluidos los servicios de telecomunicaciones, informática y conexos.

Así mismo, a lo largo de la ley, se hace referencia a la capacidad técnica y profesional de los prestadores de servicios:

- “Sólo podrán contratar con el sector público las personas naturales o jurídicas, españolas o extranjeras, que tengan plena capacidad de obrar, no estén incurso en una prohibición de contratar, y **acrediten su solvencia económica, financiera y técnica o profesional**”
- “Artículo 66. Solvencia técnica en los contratos de suministro...
 2. *En los contratos de suministro que requieran obras de colocación o instalación, la prestación de servicios o la ejecución de obras, la capacidad de los operadores económicos para prestar dichos servicios o ejecutar dicha instalación u obras **podrá evaluarse teniendo en cuenta especialmente sus conocimientos técnicos, eficacia, experiencia y fiabilidad.***

La pregunta es evidente: ¿cómo acredita una empresa la fiabilidad y calidad de sus servicios?

La respuesta no es menos evidente: de la misma forma que el CESTI da una certificación de calidad a un producto, las empresas deben presentar certificaciones acordes con su actividad.

¿ISO 20000?, ¿ISO 27001?, ¿ISO 9001?.

Sería bueno alguna indicación de la Administración en este sentido