

La acreditación, al servicio de la ciberseguridad

(Artículo publicado en la Revista Calidad de la Asociación Española para la Calidad)

José Luis Borrego Nadal

Jefe del departamento de Laboratorios y Certificación de Producto de ENAC

La información, uno de los principales activos de las compañías, ha convertido al espacio digital en su principal medio natural. Una esfera con novedosas tecnologías (el blockchain, la inteligencia artificial, la robótica, el big y smart data...), que exige una interconexión constante volviéndonos más dependientes de las infraestructuras que hacen posible el ciberespacio y más vulnerables a acciones hostiles contra dichas infraestructuras. Así, en los últimos años, se ha presentado la ciberseguridad como un elemento de especial importancia para todos los sectores, con requisitos cada vez más exigentes.

En este ámbito, las actividades de evaluación y control tienen un gran protagonismo, ya que ayudan a garantizar la seguridad, funcionalidad, operatividad y resiliencia de productos, procesos, sistemas y servicios digitales de comunicación; la seguridad, confidencialidad, integridad y disponibilidad de información y la protección de los usuarios, y a impulsar, en definitiva, un uso seguro del ciberespacio.

Sin embargo, el valor que pueden aportar estas evaluaciones a las empresas depende del buen hacer y la competencia de las entidades que las realizan. La acreditación es la herramienta que, a nivel internacional, aporta esa confianza y credibilidad, ya que solo las entidades acreditadas han demostrado a un tercero independiente, la Entidad Nacional de Acreditación en España (ENAC), mediante rigurosos procesos de evaluación, que disponen de la necesaria competencia técnica para realizar su actividad.

En este sentido, el mercado español cuenta ya con más de 50 entidades acreditadas por ENAC, que han demostrado su competencia técnica para evaluar productos y servicios relacionados con la seguridad de la información.

Ciberseguridad, clave en Europa

La importancia de la ciberseguridad ha continuado en aumento tanto a nivel europeo como en las agendas de la mayoría de los Gobiernos, ya que, en ocasiones, puede llegar a afectar a la seguridad nacional. Así, el Reglamento (UE) 2019/881, más conocido como “Cybersecurity Act”, que tiene el objetivo de reforzar la lucha contra las amenazas y ataques en materia de ciberseguridad, otorga un papel central a la acreditación para asegurar la fiabilidad y comparabilidad de las certificaciones concedidas por las diferentes entidades que operan en toda Europa y garantizar, así, la robustez del sistema y la consecución de sus objetivos. Por ello, el reglamento exige la acreditación de todas las entidades que operen en los esquemas europeos en materia de ciberseguridad con independencia de que estos sean organizaciones privadas o la propia Administración.

Dicho de otro modo, se ratifica la confianza del Parlamento y la Comisión Europea en la acreditación, herramienta a la que recurren cada vez con mayor frecuencia para aportar garantías a las actividades de evaluación de conformidad en la UE.

Una confianza también visible en los tres nuevos esquemas europeos que la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha comenzado a desarrollar en el marco del Cybersecurity Act: el Esquema de Certificación de Ciberseguridad Europeo basado en Common Criteria (EUCC), el Esquema de Certificación Europeo de Ciberseguridad en Servicios en la Nube (EUCS) y el esquema de certificación de la ciberseguridad de la UE para las redes 5G.

El primero de estos esquemas, EUCC, el más avanzado en su desarrollo ya que sustituirá al actual acuerdo europeo SOG-IS (Senior Officers Group Information Systems Security), permite el reconocimiento de certificados de seguridad de productos a los más altos niveles de exigencia en el ámbito de la Unión Europea.

En este caso, ENAC ha participado, en representación de la organización europea de acreditadores (EA), en el grupo de trabajo de ENISA que desarrolla la propuesta sobre cuáles deberán ser los requisitos de acreditación, tanto para los laboratorios de ensayo como para las entidades de certificación que realizan evaluaciones de productos dentro del esquema EUCC.

Más apoyo a las políticas públicas

Además de la mencionada Cybersecurity Act, la acreditación ha venido siendo usada desde hace tiempo en el ámbito de la ciberseguridad, como, por ejemplo, con la certificación de los sistemas de gestión de la seguridad de la información, ensayos y certificaciones de seguridad de los productos y sistemas de tecnologías de la información de acuerdo con estándares como Common Criteria o Lince, que evalúan la capacidad de un producto TIC para tratar la información de forma segura.

Asimismo, el Reglamento (UE) nº910/2014, eIDAS, para la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, ha establecido la acreditación para asegurar la competencia técnica, la operatividad e imparcialidad de los organismos que auditan y certifican a los proveedores de servicios de identificación electrónica.

A nivel nacional, el Esquema Nacional de Seguridad (ENS) fija los requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración Pública y en los servicios que los operadores privados presten a entidades públicas. Para aportar las máximas garantías, las entidades de certificación que quieran actuar en el marco de dicho esquema deben contar con la acreditación de ENAC.