ENTREVISTA

ROSALINA PORRES,

RESPONSABLE DE LOS PROCESOS DE ACREDITACIÓN EN EL ÁMBITO DE CIBERSEGURIDAD EN ENAC

"Cada vez van a presentarse más oportunidades para los evaluadores de la conformidad en el ámbito de la ciberseguridad, y nosotros, como organismo de acreditación, continuaremos trabajando para aportar confianza"

En 2024, Rosalina Porres fue galardonada por su trayectoria profesional en favor de la ciberseguridad con un premio otorgado por el Centro Criptológico Nacional (CCN). Porres cuenta con más de 25 años de experiencia en diferentes actividades de acreditación, destacando su actividad como responsable de la coordinación y supervisión de procesos de acreditación en materia de ciberseguridad y Tecnologías de la Información y la Comunicación (TIC) dentro del departamento de Laboratorios y Certificación de Producto de la Entidad Nacional de Acreditación (Enac). En las siguientes líneas, Rosalina Porres comparte su experiencia y explica el valor aportado por la infraestructura de la acreditación en el ámbito de la ciberseguridad en nuestro país y a escala europea.

Mariana Morcillo

¿Qué hitos profesionales considera que han sido clave para recibir este reconocimiento por parte del Centro Criptológico Nacional?
La mayor parte de mi carrera profesional se circunscribe al ámbito de la acreditación, formando parte del equipo técnico de la Entidad Nacional de la Acreditación desde hace 30 años. En el año 2000 mi actividad comienza a ligarse al ámbito de la ciberseguridad, convirtiéndome posteriormente en responsable de la coordinación y supervisión de procesos de acreditación en el ámbito de la ciberseguridad y TIC dentro del departamento de Laboratorios y Certificación de Producto de la Entidad Nacional de Acreditación (Enac). En estos años, he tenido la oportunidad de colaborar con las principales instituciones y autoridades de referencia del sector, tanto en nuestro país como a escala europea, en la creación de un marco de confianza en las actividades de control sobre los productos y sistemas relacionados con la seguridad de la información.

Entre mis experiencias profesionales junto al Centro Criptológico Nacional, he tenido la oportunidad de trabajar codo a codo junto a sus grandes profesionales, aportando mi apoyo en los procesos de acreditación, tanto del propio organismo de certificación como de los laboratorios de evaluación adscritos al Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI). Asimismo, he colaborado en el desarrollo y puesta en marcha del esquema de acreditación de entidades que certifican el cumplimiento del Esquema Nacional de Seguridad (ENS).

Además de mi actividad en el ámbito de la ciberseguridad a nivel nacional, he podido realizar una amplia actividad a nivel europeo, en particular, en el esquema de certificación de ciberseguridad (EUCC), basado en Common Criteria en el marco del reglamento europeo Cybersecurity Act, en cuyo desarrollo colaboré como representante de la organización europea de acreditadores European Accreditation (EA) en los grupos de trabajo de la Agencia de la Unión Europea para la Ciberseguridad, Enisa, encargados de la elaboración del esquema.

Al recibir este galardón, usted mencionó que colaborar con el Centro Criptológico Nacional ha sido un reto y un privilegio. ¿Qué aspectos concretos de esta colaboración destacaría como los más significativos para el desarrollo del sector de la ciberseguridad en España?
Para nosotros, trabajar con el CCN siempre ha sido un

"La acreditación ya aporta valor y garantías al mercado y a los consumidores en la certificación de los sistemas de gestión de la seguridad de la información, la certificación de conformidad con el ENS y ensayos de ciberseguridad en diversos ámbitos, como Internet de las Cosas (IoT) y sistemas de control industrial (IACS), entre otros"

Rosalina Porres recibió a finales de 2024 el premio a una trayectoria profesional en favor de la ciberseguridad otorgado por el Centro Criptológico Nacional (CCN).

privilegio. Poder contar con su conocimiento, experiencia y su capacidad de adaptación a las características de los procesos de acreditación, hace que la colaboración con ellos sea extremadamente valiosa.

Un ejemplo claro lo encontramos en el Esquema Nacional de Seguridad (ENS), una herramienta desarrollada en nuestro país que ha suscitado el interés de nuestros socios europeos y en el que he tenido la oportunidad de colaborar. Este esquema fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración Pública, también aplicable a operadores del sector privado, que prestan servicios o provean soluciones a entidades públicas. Para aportar las máximas garantías, se estableció la exigencia de la acreditación de Enac a las entidades certificadoras para poder actuar en el marco de dicho esquema.

Desde que los propietarios de este esquema, el Ministerio de Política Territorial y Función Pública y el CCN, se pusieron en contacto con nosotros para solicitar apoyo técnico en la integración de la acreditación para aportar las máximas garantías, la colaboración ha sido muy ágil y fluida. Así, cuando ha sido necesario, se han incluido aclaraciones o interpretaciones propuestas por Enac en las guías del CCN. Tras la aprobación de la primera revisión del esquema, se colaboró con el CCN en la definición del plan de transición para su adaptación por parte de las entidades acreditadas.

Usted ha colaborado en el desarrollo del esquema EUCC en el marco del reglamento Cybersecurity Act. ¿Cuáles son los mayores desafíos y oportunidades que percibe en la implementación de estas normativas a nivel nacional?

En mi opinión, la implementación del esquema EUCC a nivel nacional supone un desafío tanto para el CCN como para las entidades de certificación privadas a las que abre la puerta este esquema, ya que anteriormente solo certificaban los esquemas naciones. El CCN tendrá que hacer un esfuerzo para establecer la Autoridad Nacional de Certificación de la Ciberseguridad, de acuerdo con lo establecido en el artículo 58 del Reglamento (UE) 2019/881 y asumir sus funciones de supervisión.

Por otra parte, las entidades de certificación privadas que deseen trabajar en este esquema tendrán que adaptarse a una actividad novedosa para ellos. Esta apertura a la certificación privada supondrá una oportunidad para que la industria disponga de más opciones a la hora de certificar sus productos, lo que puede contribuir a acortar los tiempos de certificación de sus productos.

La regulación en ciberseguridad ha evolucionado significativamente en los últimos años. ¿Qué papel considera que juega la acreditación en este progreso y cómo contribuye Enac a su consolidación?

Las TIC forman parte de la cultura tecnológica en

la que empresas, administraciones y ciudadanos se encuentran inmersos en la actualidad; pero, además, en los últimos años, se ha presentado la ciberseguridad como un elemento de especial importancia para todos los sectores, con requisitos de seguridad cada vez más exigentes.

El espacio digital se constituye sobre una base constante de nuevas tecnologías (el blockchain, la inteligencia artificial, la robótica, el big y smart data...), haciéndonos más dependientes de las infraestructuras TIC y más vulnerables a acciones hostiles contra dichas infraestructuras. De este modo, la ciberseguridad se ha convertido en una necesidad esencial para las empresas y ciudadanos y en un objetivo prioritario en las agendas de la mayoría de los Gobiernos, ya que, en ocasiones, puede llegar a afectar a la Seguridad Nacional.

En este sentido, el papel de Enac es poner a disposición del mercado y de la administración entidades de evaluación que hayan demostrado su competencia técnica y actúen de acuerdo con normas internacionales de forma que las evaluaciones que realicen sean fiables y por tanto aporten confianza a las administraciones, las empresas y los consumidores en la seguridad de equipos y sistemas de comunicación; la seguridad, confidencialidad, integridad y disponibilidad de información; y la protección de los usuarios.

En concreto, la acreditación ya aporta valor y garantías al mercado y los consumidores en variedad de actividades tales como: la certificación de los sistemas de gestión de la seguridad de la información, la certificación de conformidad con el ENS, ensayos de ciberseguridad en diversos ámbitos tales como Internet de las Cosas (IoT) y los sistemas de control industrial (IACS), entre otros.

Los requisitos de ciberseguridad se están extendiendo a ámbitos como el IoT y los sistemas de control industrial. ¿Cómo está respondiendo Enac a estas nuevas demandas del mercado?

En los últimos años, la actividad de Enac y de todos los organismos nacionales de acreditación de la UE ha estado, y continuará estando, marcada por el enorme impacto que la reglamentación europea, debido a la confianza en el uso de la acreditación y los servicios acreditados por parte de la Administración a nivel europeo, con más de 140 legislaciones europeas que los incluyen entre sus requisitos.

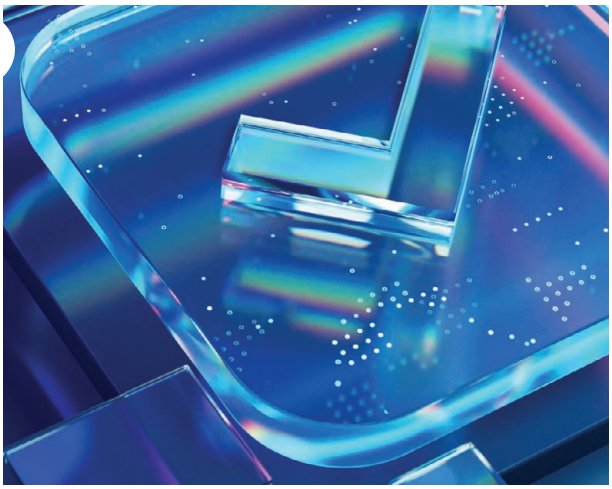
En este sentido, en el ámbito de la ciberseguridad, será necesario el desarrollo de esquemas y procesos de acreditación en reglamentos y directivas que ya han entrado en vigor o lo harán próximamente, entre los que caben destacar nuevos reglamentos enmarcados en el Nuevo Marco Legislativo (NLF) como el de Ciberresiliencia (CRA), sobre los requisitos de seguridad para los productos digitales; y el de Inteligencia Artificial, que aborda los riesgos asociados a usos específicos de la IA.

"Con cerca de 2.000 servicios acreditados que operan en la práctica totalidad de los sectores económicos, Enac pone a disposición de las empresas y del mercado español una infraestructura de evaluadores de la conformidad competentes y que disponen del máximo reconocimiento internacional"

En marco de la seguridad de productos TIC de internet de las cosas, IoT, el mercado español ya cuenta con acreditaciones tanto para ensayos como la certificación de productos, dispositivos y componentes que integran estos sistemas. Las plataformas IoT están compuestas de diversos dispositivos conectados, compuestos a su vez por diferentes componentes integrados, por ello, es esencial evaluar la ciberseguridad de componentes y dispositivos, así como de la plataforma IoT en su conjunto.

Por su parte, en el ámbito de los sistemas de control y automatización industrial (IACS), el mercado español también cuenta con servicios acreditados para ensayos de componentes (hardware y software) utilizados en sistemas de control y automatización industrial, para verificar el cumplimiento de los requisitos de la norma IEC 62443-4-2 y comprobar las capacidades que permiten a dichos componentes mitigar las amenazas para un determinado nivel de seguridad.

Además, los requisitos de ciberseguridad también van apareciendo, cada vez con más frecuencia, en diversa reglamentación sectorial, por ejemplo, en relación con la automoción, los equipos radioeléctricos o los sistemas de apuestas y juegos de casino.



Con todo ello, cada vez van a presentarse más oportunidades para los evaluadores de la conformidad en el ámbito de la ciberseguridad, y nosotros, como organismo de acreditación, continuaremos trabajando para aportar confianza tanto al mercado como a las administraciones públicas en aquellos ámbitos necesarios.

Con el avance de tecnologías como la inteligencia artificial, ¿qué papel desempeñará Enac en la certificación de sistemas que incorporen estas tecnologías?

Durante la preparación del proyecto de Reglamento de la UE sobre inteligencia artificial, Enac ha participado en el grupo de trabajo de la organización europea de acreditadores, European Accreditation, dedicado a trasladar sugerencias a la Comisión Europea sobre el uso de servicios acreditados en aquellos ámbitos de la disposición que puedan requerir aportar la máxima confianza en las actividades de evaluación y control de los sistemas de inteligencia artificial puestos a disposición del mercado, las autoridades y los consumidores europeos.

Por su parte la Agencia de la Unión Europea para la Ciberseguridad (Enisa), también ha trasladado sus comentarios al anteproyecto de reglamento sobre los ámbitos en los que la IA podría ser objeto de una certificación de ciberseguridad y está realizando un trabajo previo de evaluación sobre cómo podrían reutilizarse los esquemas de certificación que se están elaborando en el marco del Cybersecurity Act.

La marca Enac es reconocida en más de 120 países. ¿Cómo influye esta proyección internacional en el fortalecimiento de la confianza en los sistemas y productos españoles?

Abrirse paso en los mercados exteriores representa en muchas ocasiones un reto, ya que, a la propia competencia de las empresas locales y a las imposiciones económicas aduaneras se le unen barreras de tipo técnico que exigen que los productos cumplan una serie de requisitos generalmente asociados a características de seguridad, protección del medioambiente o calidad, conocidos como Obstáculos Técnicos al Comercio (OTC).

Los obstáculos técnicos al comercio surgen por los diferentes requisitos técnicos exigidos a los productos en cada país, ya sean requisitos reglamentarios que pretenden proteger la seguridad de consumidores y medioambiente, o normas voluntarias que definen generalmente las características de calidad que debe cumplir el producto para satisfacer a los compradores. Esto obliga al fabricante a adaptar sus productos a las diferentes exigencias y a demostrar que son conformes con dichas reglamentaciones.

Sin embargo, en muchas ocasiones, el obstáculo no radica tan solo en la adaptación del producto a las exigencias técnicas de otro mercado, o a la evaluación de la conformidad del producto con las reglamentaciones técnicas. También se observa una falta de confianza del propio mercado (las autoridades, importadores, clientes, etc.) en los certificados que acompañan a los productos para avalar su conformidad, y que son emitidos por laboratorios, entidades de inspección y certificación, y verificadores en el país de origen del producto, el país desde el que se exporta.

La falta de confianza puede traer consigo que el producto tenga que ser evaluado en cada uno de los países destino, independientemente de que lo haya sido en el país de origen, incluso si la evaluación se ha realizado conforme a los requisitos del país importador.

Para superar y minimizar las barreras, la práctica totalidad de los países han establecido organismos nacionales de acreditación, al ser la acreditación uno de los mecanismos reconocidos por la Organización Mundial del Comercio y la Unión Europea para minimizar estos obstáculos.

En Europa, la relevancia dada a esta actividad queda patente con la aprobación del Reglamento (CE) nº765/2008 que requiere a cada Estado miembro que designe a un único Organismo Nacional de Acreditación dotado de potestad pública para otorgar acreditaciones y establece los requisitos que deben cumplir tanto en su estructura como en su funcionamiento. En España, dicha designación recae en la Entidad Nacional de Acreditación a través del Real Decreto 1715/2010.

Con cerca de 2.000 servicios acreditados que operan en la práctica totalidad de los sectores económicos, Enac pone a disposición de las empresas y del mercado español una infraestructura de evaluadores de la conformidad competentes y que disponen, a través de la acreditación de Enac, del máximo reconocimiento internacional. ●