Nota de Prensa

DORA marca un camino común para la gobernanza tecnológica y la gestión del riesgo en el sector financiero

- AENOR y Trend Micro reúnen a expertos para abordar cómo la regulación se convierte en palanca de resiliencia y eficiencia para el sector financiero.

Madrid, 19 de noviembre de 2025.- En un contexto de creciente exposición a las ciberamenazas, AENOR, entidad líder en generación de confianza, y Trend Micro, líder mundial en ciberseguridad, han reunido a referentes del sector financiero en un workshop exclusivo para debatir cómo el Reglamento de Resiliencia Operativa Digital (DORA) está transformando la gobernanza tecnológica y la gestión del riesgo.

El encuentro, inaugurado por Rafael García Meiro, CEO de AENOR, y Toni Abellán, Country Manager de Trend Micro en España, ha analizado los retos y oportunidades que DORA representa para un sector que, según los últimos informes de Trend Micro, se ha convertido en uno de los principales objetivos de los ciberataques a nivel mundial.

Durante su intervención, Rafael García Meiro destacó el papel de la certificación como eje esencial de la confianza digital. “Cuanto más confiamos en la tecnología, más necesitamos de la ciberseguridad. En AENOR trabajamos para identificar las mejores prácticas y reforzar la seguridad del modelo de gobernanza tecnológica. La certificación es un elemento diferenciador que aporta confianza, simplifica el cumplimiento normativo y fortalece la seguridad jurídica de las organizaciones”, ha afirmado.

Por su parte, Toni Abellán, Country Manager de Trend Micro en España, ha subrayado la necesidad de entender DORA como una oportunidad estratégica. “La regulación debe habilitar el negocio, no limitarlo. DORA nos impulsa hacia una ciberseguridad más proactiva y estratégica, en la que el CISO forme parte del núcleo de las decisiones corporativas. La ciberseguridad debe ser el denominador común que trace un camino seguro para todas las compañías del sector financiero”, ha señalado.

La jornada ha incluido un panel de expertos que ha contado con la participación de Silvia Senabre, Jefa del Grupo de Riesgo Tecnológico del Banco de España; Maribel de la Vega, presidenta de la Comisión de Auditoría de Nationale-Nederlanden España; Rafael Vergara, Category Manager de Soluciones en Digitalización y Tecnología de AENOR; y Raúl Guillén, evangelizador de Trend Micro.

Durante la sesión, han coincidido en que DORA marca un antes y un después en la gestión del riesgo tecnológico, ofreciendo un marco común que permitirá homogeneizar la resiliencia operativa en toda la cadena de valor.

“DORA da un paso decisivo para armonizar los requisitos de resiliencia en el sector financiero, ofreciendo una visión de conjunto que refuerza la cooperación entre entidades y proveedores”, ha explicado Senabre. En la misma línea, Maribel de la Vega ha apuntado que “la norma impulsa la integración de la tecnología en la estrategia de negocio, visibilizando los riesgos tecnológicos y asegurando la asignación de recursos adecuados para mitigarlos”.

Para Rafael Vergara, la regulación “armoniza los estándares de seguridad y crea un lenguaje común que incrementa la eficiencia y transparencia en el sector”. Finalmente, Raúl Guillén ha destacado que “representa una oportunidad para construir un modelo de ciberseguridad más maduro y sostenible, capaz de anticipar amenazas y generar valor para las organizaciones”.

El encuentro también ha subrayado la urgencia de reforzar la monitorización continua de la seguridad, promover una mayor concienciación a nivel directivo habilitando la comprensión del idioma del riesgo, fortalecer la colaboración entre entidades, aseguradoras y proveedores tecnológicos para compartir buenas prácticas y elevar los estándares de seguridad a todos sectores críticos de la cadena de valor.

Y es que, de acuerdo con los datos de Trend Micro, el sector bancario es uno de los más afectado por incidentes de ciberseguridad, impulsados por vulnerabilidades en la nube, configuraciones incorrectas y riesgos derivados de terceros y proveedores. Estos datos refuerzan la necesidad de una gobernanza tecnológica sólida y una regulación homogénea, pilares sobre los que se asienta el Reglamento DORA.

Para abordar los requisitos establecidos en DORA la ISO 27001:2022 es una buena base de comienzo, ya que establece un sistema de gestión de la seguridad de la información que integra procesos críticos como la identificación y el tratamiento de riesgos, la protección de activos digitales o la gestión de incidentes. Estos elementos son esenciales para garantizar la resiliencia operativa que exige la regulación y es por ello que AENOR considera este referencial internacional como necesario dentro de su Certificación de DORA. Al adoptar la ISO 27001, las organizaciones disponen de un marco probado y reconocido internacionalmente que les permite estructurar controles, políticas y procedimientos alineados con las obligaciones regulatorias, reduciendo la complejidad y acelerando el cumplimiento. Por todo ello, la certificación DORA de AENOR busca ofrecer, en el ámbito de aplicación del reglamento, una herramienta para fortalecer la resiliencia operativa digital conforme al cumplimento del nuevo marco europeo.

Ante este escenario en el que los ciberataques crecen a un ritmo sin precedentes, DORA se consolida como una respuesta necesaria y transformadora, que permite alinear tecnología, negocio y regulación.

Más allá del cumplimiento, el reglamento ofrece una hoja de ruta para convertir la resiliencia operativa en una ventaja competitiva, reforzando la confianza y la estabilidad del ecosistema financiero europeo.

Sobre AENOR

AENOR contribuye a la transformación de la sociedad creando confianza entre organizaciones y personas, mediante servicios de evaluación de la conformidad (certificación, inspección y ensayos), formación e información; además de la consultoría de transformación de negocio que desarrolla la sociedad AENOR Conocimiento. Es la entidad líder en generación de confianza de España y más de 91.000 centros de trabajo en el mundo tienen alguno de los certificados de AENOR en campos como la Gestión de la Calidad, la Inteligencia Artificial, la Ciberseguridad o los relacionados con los criterios ESG, como pueden ser el *Compliance* penal, el buen gobierno corporativo, la Igualdad, la gestión ambiental o la construcción sostenible.

Entre las ventajas competitivas diferenciales de AENOR se encuentran el reconocimiento de marca más elevado entre las empresas y los consumidores; contar con personal propio, lo que le permite gestionar el conocimiento acumulado en beneficio de sus clientes; innovar en la resolución de nuevas brechas de competitividad gracias a su proximidad con las fuentes de conocimiento; y su capilaridad geográfica y sectorial.

AENOR es una entidad global, que ya desarrolla operaciones en 87 países. En España dispone de sedes en todas las Comunidades Autónomas, con auditores propios, y tiene presencia permanente en otros 12 países, principalmente de Latinoamérica y Europa.

Para más información:
Quique Cervera Garbayo
Responsable de la relación con los medios
Tel.: + 34 630 47 01 26
qcervera.ext@aenor.com
Síguenos en:

Sobre Trend Micro

Trend Micro, líder mundial en ciberseguridad, contribuye a que el mundo sea un lugar más seguro, blindando el intercambio de información digital entre personas, gobiernos y empresas.

La compañía aprovecha su experiencia en seguridad y la inteligencia artificial para proteger a más de 500.000 empresas y millones de personas en la nube, la red, endpoints y dispositivos de todo el mundo.

En el centro se encuentra Trend Vision One™, la única plataforma de ciberseguridad empresarial basada en inteligencia artificial que permite administrar la gestión de la exposición a los riesgos cibernéticos y las operaciones de seguridad, proporcionando una protección por capas en entornos locales, híbridos y multicloud.

La inigualable inteligencia sobre amenazas que ofrece Trend ayuda a las organizaciones a defenderse de forma proactiva contra cientos de millones de amenazas cada día.

Con 7.000 empleados en 70 países, Trend ofrece a los responsables de seguridad adelantarse a las amenazas, con resultados de seguridad proactivos en toda la superficie de ataque. Esto incluye entornos críticos como AWS, Google, Microsoft y NVIDIA. La seguridad proactiva comienza aquí TrendMicro.com