

La protección del sector financiero de la UE: expectativas y prioridades desde la perspectiva de la SRI

ENISA acaba de publicar un [estudio](#) sobre la seguridad de las redes y de la información (SRI) en el sector financiero de la UE, con información sobre el panorama normativo y las prioridades del sector a nivel estratégico y de gobernanza.

Este estudio tiene como finalidad entender y comparar las obligaciones relevantes para la seguridad de la información dentro el sector financiero en la mayoría de los 28 Estados miembros de la UE; compararlas con las expectativas del sector; y extraer una visión clara de las prioridades importantes para el futuro.

El estudio también busca comprender las diferencias entre los objetivos de las normativas y las prioridades del sector, y poner de relieve los diferentes enfoques de los 28 Estados miembros de la UE con relación a la supervisión de la SRI. El trabajo parte de una labor de inventario consistente en:

1. La identificación de los requisitos de SRI a nivel nacional.
2. Entrevistas con autoridades supervisoras financieras nacionales, autoridades europeas y representantes del sector.

El informe pone de relieve varios objetivos deseables:

- La convergencia de las prácticas de supervisión en cuestiones relativas a la SRI.
- La necesidad de disponer de unas directrices claramente definidas por lo que respecta a la conformidad y a las buenas prácticas.
- La necesidad de mejorar la cooperación proactiva para afrontar los retos de la SRI.

Según el estudio, los grandes grupos bancarios internacionales muestran una buena comprensión del paisaje de riesgos y de los programas de seguridad disponibles. Muchos bancos han introducido unas buenas prácticas optimizadas, especialmente en el campo de la gobernanza de TI, mientras que los agentes medianos demuestran una implicación y una capacidad limitadas por parte de sus equipos directivos en cuanto a la obtención de certificaciones con arreglo a las actuales normas internacionales, así como una pérdida de prioridad de las inversiones en materia de seguridad. Cabía esperar diferencias como estas. El objetivo es entender en qué medida dichas perspectivas podrían deteriorar la resiliencia financiera en su conjunto.

16/01/2015

EPR01/2015

www.enisa.europa.eu

El profesor [Udo Helmbrecht](#), Director Ejecutivo de ENISA, comentó: *“La protección del ciberespacio y de las comunicaciones electrónicas se ha convertido en una prioridad gubernamental y sectorial en todo el mundo. La creciente relevancia que las tecnologías de la información y de la comunicación tienen en las funciones esenciales de la economía ha reforzado la necesidad de adoptar medidas de prevención y protección en todos los sectores, incluido, naturalmente, el sector financiero. ENISA continuará contribuyendo a la mejora de los criterios básicos de la seguridad de la información y apoyando las iniciativas de cooperación en el sector financiero a través de sus conocimientos. Para ello, apoyará al Banco Central Europeo y a las autoridades del sector financiero en la organización de pruebas de resistencia, garantizará un uso seguro de los servicios basados en la nube y desarrollará una guía sobre medidas de seguridad paneuropeas”*.

El informe está destinado principalmente a responsables de seguridad informática, directores de sistemas informáticos y directores técnicos del sector financiero, expertos en SRI de las autoridades supervisoras financieras nacionales, expertos en SRI en Sistemas Europeos de Supervisores Financieros (SESF), como la AEB, la AEVM y la AESPJ, y asociaciones profesionales. Asimismo, se proponen una serie de recomendaciones con relación al futuro de la SRI en el sector financiero, y se facilita información de referencia de alto nivel sobre cuestiones específicas del Sistema Financiero Europeo.

Informe completo: [La seguridad de las redes y de la Información en el sector financiero: panorama normativo y prioridades del sector](#)

Consultas y entrevistas: Lionel Dupre, experto en SRI de ENISA, **correo electrónico:** lionel.dupre@enisa.europa.eu, **móvil:** +30 6948460132