JERS
Junta Europea de Riesgo Sistémico
Sistema Europeo de Supervisión Financiera

Nota de prensa

16 de abril de 2024

La JERS publica un informe sobre las herramientas operacionales para la ciberresiliencia

Como parte de su estrategia macroprudencial para aumentar la ciberresiliencia del sistema en su conjunto, la Junta Europea de Riesgo Sistémico (JERS) ha publicado hoy un informe que se centra en tres grupos de herramientas operacionales:

1 **Las herramientas para la recopilación, el intercambio y la gestión de información** proporcionan datos de alta calidad para realizar seguimientos, calibrar herramientas y gestionar ciberincidentes sistémicos *ex post*. Estas herramientas, así como los centros de notificación de ciberincidentes, son fundamentales para un mecanismo de intercambio de información a escala de la UE.

2 **Las herramientas de coordinación** ayudan a las autoridades y a las instituciones financieras a mitigar los posibles efectos negativos para la estabilidad financiera asegurando una respuesta común eficaz para todas las partes involucradas. La aplicación en curso del marco paneuropeo de coordinación de ciberincidentes sistémicos (EU-SCICF, por sus siglas en inglés) permitirá mejorar notablemente los esfuerzos en este ámbito.

3 **Los sistemas de emergencia y de respaldo (*backup*)** que se han establecido para contribuir a garantizar la continuidad de funciones económicas esenciales, incluso en situaciones de emergencia grave.

En este contexto, las instituciones públicas y privadas pueden considerar tres posibles vías:

1 mejorar la gestión de la información y las iniciativas para intercambiar información;
2 alinear las prácticas de gestión y coordinación de crisis, y
3 considerar las ventajas y los inconvenientes de las opciones para casos de contingencia y de los mecanismos de respaldo de todo el sistema.

El informe se basa en los exhaustivos trabajos llevados a cabo por la JERS sobre cómo mitigar los riesgos derivados de un ciberincidente sistémico. El primer informe de la JERS sobre ciberriesgo sistémico establece los fundamentos conceptuales de una respuesta macroprudencial a este riesgo. El informe sobre mitigación del ciberriesgo sistémico incluye la base del enfoque con

Junta Europea de Riesgo Sistémico
Dirección General de Comunicación
Sonnemannstrasse 20, 60314 Frankfurt am Main, Alemania
Tel.: +49 69 1344 7455, correo electrónico: media@esrb.europa.eu, sitio web: www.esrb.europa.eu

objetivos de tolerancia a impactos sistémicos (SITO, por sus siglas en inglés) con el fin de definir los umbrales a partir de los cuales puede ser necesario adoptar medidas de política macroprudencial para evitar un impacto severo en el sector financiero. En el informe sobre los avances en las herramientas macroprudenciales para la ciberresiliencia se evalúan las medidas preventivas y correctivas a disposición de las autoridades, entre ellas el uso de colchones de capital y las pruebas de ciberresiliencia a través del análisis de escenarios (CyRST, por sus siglas en inglés).

La JERS continuará trabajando en la elaboración de una ciberestrategia macroprudencial integral, que también será acorde con la implantación del Reglamento sobre resiliencia operativa digital (DORA, por sus siglas en inglés). Actualmente, la JERS está poniendo a prueba el enfoque SITO, revisando los desarrollos recientes en el ámbito de las CyRST y también analizando más detalladamente las sinergias resultantes de la combinación de herramientas operacionales y financieras. El European Systemic Cyber Group (grupo de trabajo europeo de ciberriesgo sistémico), continuará actuando como un *hub* para las autoridades macroprudenciales del Espacio Económico Europeo, en colaboración con el Banco de Inglaterra.

Persona de contacto para consultas de los medios de comunicación: Clara Martín Marqués, tel.: +49 69 1344 17919.

Junta Europea de Riesgo Sistémico
Dirección General de Comunicación
Sonnemannstrasse 20, 60314 Frankfurt am Main, Alemania
Tel.: +49 69 1344 7455, correo electrónico: media@esrb.europa.eu, sitio web: www.esrb.europa.eu