NOTAS OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA

FUNCAS – 1 de diciembre de 2022 **ODF – Funcas 84 / 2022**

Nueva regulación para la ciberseguridad de las empresas financieras europeas

A medida que el ecosistema financiero se hace más digital, protegerlo de los ataques cibernéticos y del fraude es vital para asegurar la estabilidad financiera. Desde la Unión Europea se siguen dando pasos para hacer el sistema financiero europeo más resiliente en este contexto.

El Parlamento Europeo acaba de aprobar un conjunto de estrictas reglas sobre ciberseguridad para las empresas financieras, incluidas las plataformas de criptomonedas[1]. El cuerpo normativo, impulsado desde la Comisión, se ha denominado "Ley de resiliencia operativa digital"[2] (Dora, por sus siglas en inglés). Esta normativa pretende convertirse en una piedra angular para el desarrollo de las finanzas digitales en la Unión Europea. Nace con la idea de apoyar la innovación, pero también hacerla segura. Se busca proteger a los inversores europeos y preparar a las empresas financieras contra los ataques cibernéticos. Y es que el coste global de los ataques cibernéticos para todas las empresas a escala mundial alcanzará los 10,5 billones anuales para 2025, frente a los 3 billones de 2015.

En particular, la nueva regulación establece un conjunto común de estándares para gestionar los riesgos digitales en todo el sector financiero y garantizar que se implementen las medidas necesarias para protegerse contra los ataques cibernéticos. Las instituciones financieras tendrán que supervisar y reportar los incidentes cibernéticos. También

[1] EU Lawmakers Vote for Stronger Cyber Protection for Crypto, Other Finance. CoinDesk. 10 noviembre 2022. https://www.coindesk.com/policy/2022/11/10/eu-lawmakers-vote-stronger-cyber-protection-for-crypto-other-finance/

[2] Reglamento sobre la resiliencia operativa digital del sector financiero. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

estarán obligadas a disponer de marcos internos de gobernanza y control que garanticen una gestión eficaz y prudente de todos los riesgos tecnológicos.

Además, deberán someterse a pruebas periódicas de resiliencia operativa digital. Todos los sistemas y aplicaciones tecnológicos esenciales se probarán al menos una vez al año. También se realizarán pruebas avanzadas, que se llevarán a cabo cada tres años.

Esta normativa no solo obliga a las entidades tradicionales. Las grandes tecnológicas proveedoras de servicios a las instituciones financieras también tendrán que someterse a supervisión. Por tanto, con la aplicación de Dora, los terceros proveedores tecnológicos, que antes no estaban regulados, ahora quedarán bajo la supervisión de los reguladores, al menos en lo que a riesgos operativos se refiere.

Dado el cambio significativo que supone la nueva regulación, se ha previsto un periodo de gracia de 24 meses para que las empresas se pongan al día con la nueva normativa. En cualquier caso, el tiempo y, sobre todo, el ciber-riesgo apremian al sector financiero a avanzar para ganar en resiliencia operativa.