El reglamento DORA, la nueva estrategia de la UE para reforzar la ciberseguridad del sector financiero

Análisis Flash ESYS | Raquel Jorge Ricart y Laura Torres Saavedra
– septiembre 2022

En los próximos meses antes de terminar 2022 se espera que el reglamento DORA sea aprobado. Es una regulación estratégica tanto para la seguridad como para la competitividad económica y el respeto a los derechos de la Unión Europea. Es importante observar tanto sus objetivos como los mecanismos de gobernanza que va a llevar a cabo.

El reglamento en Resiliencia Operativa Digital, "DORA" por sus siglas en inglés, va a ser una regulación, no solo estratégica, sino también crítica, para la seguridad, competitividad económica y garantía de los derechos fundamentales de la Unión Europea.

Es una regulación que puede suponer un antes y un después, puesto que hasta ahora no ha habido una efectiva coordinación en todo el ciclo de gestión de la ciberseguridad para las entidades financieras ubicadas a lo largo de la Unión Europea: ni en la forma en que se abordaba el ciclo (identificación, protección, prevención, respuesta y recuperación) ni en una comunicación ni cohesión de las políticas públicas y gestión de crisis entre sectores y entre Estados miembros.

La relevancia y carácter crítico de esta regulación, de la que se espera quede aprobada en noviembre de 2022, es su objetivo de mejorar la resiliencia y capacidad de respuesta de entidades financieras frente ataques cibernéticos e incidentes de las TICs. Ahora bien, el objetivo de DORA va más allá de la perspectiva puramente técnica. También va a suponer cambios en la gobernanza: en la relación con los terceros proveedores y en las nuevas responsabilidades de los órganos de Dirección.

Algunos de los aspectos principales de este acuerdo es que DORA busca regular el sistema de notificación de incidentes TIC mediante la siguiente vía: las empresas deben informar a sus usuarios y clientes cuando el incidente tenga o pueda tener un impacto en sus intereses financieros y ahora tendrán también el requisito de notificar a las autoridades competentes aquellas interrupciones TIC graves.

También, la presidencia del Consejo y el Parlamento Europeo, ya en su acuerdo técnico de julio de 2022, garantizaron en el texto que dentro de los próximos dos años se establecerá una única plataforma a nivel europeo para notificar incidentes graves del servicio de Tecnologías de la Información (IT).

Por otro lado, los proveedores IT, incluidos los de la nube, deberán tener sede en el territorio de la Unión Europea y estarán bajo la observación de las Autoridades Europeas de Supervisión (AES). Las AES les podrán enviar recomendaciones, realizar inspecciones, tanto presenciales como en línea e imponer sanciones cuando lo encuentren necesario. También, tendrán la capacidad de solicitar información a estas empresas para estar al tanto de cualquier cambio en su estructura administrativa.

Los colegisladores han basado el reglamento en normas técnicas europeas reconocidas a nivel internacional y en buenas prácticas del sector. Estas giran en torno a funciones específicas en la gestión de riesgos TIC tales como identificación, protección, prevención, respuesta y recuperación.

Bruselas ha precisado que las entidades financieras deberán tener una política de continuidad de la actividad operativa. Esta incluirá sistemas y herramientas que minimicen el impacto de riesgo TIC, identifiquen fuentes de riesgo y establezcan medidas de protección, prevención y detección de actividades anómalas.

Asimismo, el Parlamento Europeo contempla la seguridad y resiliencia de las infraestructuras e instalaciones físicas que sustentan el uso de la tecnología como parte de la huella digital de las operaciones de una entidad financiera.

Siguientes pasos

Si los tiempos se cumplen, se espera que la regulación DORA quede aprobada en noviembre de 2022. Una vez entre en vigor, los Estados Miembros tendrán 21 días para trasponer los nuevos elementos de la regulación a nivel nacional.

La reglamentación aplicará a entidades financieras reguladas a nivel europeo tales como bancos, intermediarios de seguros, firmas de inversión, entidades de dinero electrónico, proveedores de servicios IT, proveedores de nube, auditores legales, sociedades de gestión, agencias de calificación, entre otros.

En ese sentido, varios retos -y, por tanto, oportunidades- se presentan para la efectiva implementación, ejecución y gestión de la regulación DORA:

- Capacitar a las entidades financieras de adecuados canales de comunicación para la notificación de incidentes;

- Fomentar una “cultura de ciberseguridad” realmente integral, que conciba DORA no solo como una regulación que cumplir al uso, sino también una forma de transformar las organizaciones en su conjunto para ser resilientes en el largo plazo, de manera eficiente y que permee desde las altas direcciones de las empresas hasta los puestos más tácticos dentro de la organización.

- Establecer una publicación periódica -anual o cada dos años- donde se reporten los aprendizajes y lecciones más importantes de la implementación de DORA en sí, y de las enseñanzas, mejoras y retos que han experimentado las entidades del sector financiero tras hacer uso de ella.

Todo ello permitirá mejorar la regulación, así como la propia vida de las empresas en un mundo cada vez más digitalizado. Estas medidas son un pilar fundamental que ayudará a la UE y a sus actores a ser más resilientes y seguir apoyando el bienestar económico y social de la región.