Banca / Bancos Centrales

Resiliencia en la banca, también en el plano de los ciberriesgos

Expansión (España)

Virginia Marcos

La ciberseguridad se ha convertido en una prioridad estratégica de los principales organismos globales encargados de velar por la estabilidad financiera como el Consejo de Estabilidad Financiera (FSB por sus siglas en inglés) o el Comité de Supervisión Bancaria de Basilea, así como de las autoridades bancarias en la Unión Europea (UE): la Autoridad Bancaria Europea, el Banco Central Europeo (BCE), y a nivel nacional, el Banco de España.

Este impulso para hacer frente a los ciberriesgos en los últimos años se engloba dentro de la creciente relevancia y atención de las autoridades hacia los riesgos operacionales a los que está expuesta una entidad financiera, con sus implicaciones para la estabilidad financiera. Pero también, promovido por el fuerte incremento de los ciberincidentes, con la banca como uno de los sectores altamente expuestos a los riesgos cibernéticos. De hecho, según el Banco de España, el número de ciberincidentes se ha duplicado entre 2018 y 2022 en el sector financiero a nivel global y se espera una tendencia alcista. Ello puede deberse a factores estructurales como son la progresiva digitalización del sector; así como coyunturales, por el aumento de las tensiones geopolíticas globales.

Esta línea de trabajo se está materializando en nuevos requerimientos regulatorios y prioridades de supervisión, específicamente en la UE, el Reglamento de Ciberseguridad conocido como DORA y un ejercicio de resiliencia cibernética al sector bancario. Precisamente, fue hace unas semanas cuando el BCE publicó los resultados del primer ejercicio de ciberresiliencia, y que se enmarcan dentro de lo que este denomina las pruebas de estrés temáticas. Estos ejercicios versan sobre un riesgo específico y se realizan cada dos años (en 2022 fue un estrés climático), alternados con aquellos de estrés macrofinanciero habituales a la banca europea.

El punto de partida de este ejercicio de resistencia frente a los ciberriesgos es el de la materialización de un ciberataque severo, con impacto en la operativa diaria de la entidad. En este sentido, se testea la capacidad de los bancos de afrontar el ciberataque, evaluando las medidas llevadas a cabo para retornar a la normalidad. Esta capacidad de respuesta es entendida en un rango amplio, ya que van desde medidas de recuperación hasta planes de contingencia y medidas de emergencia.

En el ejercicio han participado 109 bancos europeos (de las 113 entidades supervisadas directamente por el BCE), distinguiendo dos niveles de análisis: uno estándar para la mayor parte de bancos (81 entidades), formado por un cuestionario y proporcionando evidencias de políticas internas y procedimientos para hacer frente a ciberriesgos, así como resultados de pruebas de recuperación realizadas similares a las del escenario propuesto por el supervisor; y otro análisis adicional a 28 entidades, que además de lo solicitado en el estándar, incluye un ejercicio de resistencia cibernética con las evidencias correspondientes de una recuperación satisfactoria.

La prueba de resistencia no mide la capacidad para prevenir ciberataques, se centra en evaluar cómo los bancos responden y su capacidad de recuperación. Los resultados, principalmente cualitativos, se han comunicado a las entidades a nivel individual, con un informe específico y recomendaciones. Además, el BCE ha notificado que incluirá los resultados como parte de su proceso anual revisión y evaluación supervisora (SREP) de este 2024, que evalúa el perfil de riesgos de cada entidad. Sin embargo, en este caso, y a diferencia del estrés tradicional financiero, los resultados del ciberestrés no afectarán a los requerimientos de capital de los bancos.

Con ello, según el propio BCE, los bancos europeos han demostrado que tienen capacidad de respuesta y recuperación ante potenciales ciberataques, aunque existen áreas de mejora (desde valoración de la dependencia de proveedores externos críticos a estimar las pérdidas directas e indirectas de un ciberataque) que les permitan ser más resilientes ante los ciberriesgos y garantizar la continuidad del negocio.

De esta forma, apoyando la resiliencia en el mundo de los ciberriesgos se avanza un paso hacia una banca más estable, con una base tecnológica sólida para proseguir en su transformación digital, proceso vital en el que se encuentra inmerso el sector para mejorar su eficiencia y competitividad.

AVISO LEGAL

El presente documento no constituye una "Recomendación de Inversión" según lo definido en el artículo 3.1 (34) y (35) del Reglamento (UE) 596/2014 del Parlamento Europeo y del Consejo sobre abuso de mercado ("MAR"). En particular, el presente documento no constituye un "Informe de Inversiones" ni una "Comunicación Publicitaria" a los efectos del artículo 36 del Reglamento Delegado (UE) 2017/565 de la Comisión de 25 de abril de 2016 por el que se completa la Directiva 2014/65/UE del Parlamento Europeo y del Consejo en lo relativo a los requisitos organizativos y las condiciones de funcionamiento de las empresas de servicios de inversión ("MiFID II").

Los lectores deben ser conscientes de que en ningún caso deben tomar este documento como base para tomar sus decisiones de inversión y que las personas o entidades que potencialmente les puedan ofrecer productos de inversión serán las obligadas legalmente a proporcionarles toda la información que necesiten para esta toma de decisión.

El presente documento, elaborado por el Departamento de BBVA Research, tiene carácter divulgativo y contiene datos u opiniones referidas a la fecha del mismo, de elaboración propia o procedentes o basadas en fuentes que consideramos fiables, sin que hayan sido objeto de verificación independiente por BBVA. BBVA, por tanto, no ofrece garantía, expresa o implícita, en cuanto a su precisión, integridad o corrección.

El contenido de este documento está sujeto a cambios sin previo aviso en función, por ejemplo, del contexto económico o las fluctuaciones del mercado. BBVA no asume compromiso alguno de actualizar dicho contenido o comunicar esos cambios.

BBVA no asume responsabilidad alguna por cualquier pérdida, directa o indirecta, que pudiera resultar del uso de este documento o de su contenido.

Ni el presente documento, ni su contenido, constituyen una oferta, invitación o solicitud para adquirir, desinvertir u obtener interés alguno en activos o instrumentos financieros, ni pueden servir de base para ningún contrato, compromiso o decisión de ningún tipo.

INTERESADOS DIRIGIRSE A:
BBVA Research: Calle Azul, 4. Edificio La Vela – 4ª y 5ª planta. 28050 Madrid (España).
Tel.:+34 91 374 60 00 y +34 91 537 70 00 / Fax:+34 91 374 30 25
www.bbvaresearch.com