La ciberseguridad de los bancos - Una segunda generación de enfoques regulatorios



La ciberseguridad de los bancos: una segunda generación de enfoques regulatorios

Resumen ejecutivo

La resiliencia cibernética sigue siendo una prioridad para la industria de servicios financieros y un área clave de atención para las autoridades financieras. Esto no es sorprendente dado que los incidentes cibernéticos representan una amenaza significativa para la estabilidad del sistema financiero y la economía global. El sistema financiero realiza una serie de actividades clave que apoyan la economía real (por ejemplo, toma de depósitos, préstamos, pagos y servicios de liquidación). Los incidentes cibernéticos pueden interrumpir las tecnologías de información y comunicación que respaldan estas actividades y pueden conducir al mal uso y abuso de los datos que dichas tecnologías procesan o almacenan. Esto se complica por el hecho de que el panorama de las amenazas cibernéticas sigue evolucionando y volviéndose más complejo en medio de la digitalización continua, el aumento de las dependencias de terceros y las tensiones geopolíticas. Además, el costo de los incidentes cibernéticos ha aumentado continua y significativamente a lo largo de los años.

Este documento actualiza Crisanto y Prenio (2017) revisando las regulaciones cibernéticas en las jurisdicciones cubiertas en ese documento, así como examinando las emitidas en otras jurisdicciones. Además de las regulaciones cibernéticas en la RAE de Hong Kong, Singapur, el Reino Unido y los Estados Unidos, que cubrió el documento de 2017, este documento examina las regulaciones cibernéticas en Australia, Brasil, la Unión Europea, Israel, Kenia, México, Perú, Filipinas, Ruanda, Arabia Saudita y Sudáfrica. Las jurisdicciones fueron elegidas para reflejar las regulaciones cibernéticas tanto en las economías avanzadas (EA) como en las economías de mercados emergentes y en desarrollo (EMED). Esto pone de relieve el hecho de que desde 2017 varias jurisdicciones, incluidas las EMED, han establecido regulaciones cibernéticas.

Quedan dos enfoques predominantes para la regulación de la resiliencia cibernética de los bancos: el primero aprovecha las regulaciones relacionadas existentes y el segundo implica la emisión de regulaciones integrales. El primer enfoque toma como punto de partida las regulaciones sobre riesgo operativo, seguridad de la información, etc. y les agrega elementos ciber específicos. Aquí, el riesgo cibernético se considera como cualquier otro riesgo y, por lo tanto, también se aplican los requisitos generales para la gestión de riesgos, así como los requisitos sobre seguridad de la información y riesgos operativos. Este enfoque se observa más comúnmente en jurisdicciones que ya tienen estas regulaciones relacionadas firmemente establecidas. El segundo enfoque busca cubrir todos los aspectos de la ciberseguridad, desde los acuerdos de gobernanza hasta los procedimientos operativos, en una regulación global. En ambos enfoques, para contrarrestar los riesgos que podrían resultar de tener demasiada prescriptividad en las regulaciones cibernéticas, algunas regulaciones combinan principios generales de resiliencia cibernética con un conjunto de requisitos básicos. Independientemente del enfoque regulador adoptado, el principio de proporcionalidad se tiene debidamente en cuenta en la aplicación de los marcos de ciberresiliencia.

Ya sea como parte de regulaciones relacionadas o integrales separadas, las políticas recientes de seguridad cibernética han evolucionado y podrían describirse como regulaciones cibernéticas de "segunda generación". Las regulaciones cibernéticas de "primera generación", que se emitieron principalmente en AE, se centraron en establecer un enfoque y controles de gestión de riesgos cibernéticos. En los últimos años, las autoridades, incluidas las de EMED, han emitido regulaciones cibernéticas nuevas o adicionales. Estas regulaciones de segunda generación tienen una mentalidad más arraigada de "asumir incumplimiento" y, por lo tanto, están más alineadas con los conceptos de resiliencia operativa. Como tales, se centran en mejorar la resiliencia cibernética y proporcionar a las instituciones financieras y autoridades herramientas específicas para lograrlo.

Las regulaciones de "segunda generación" aprovechan los enfoques de políticas existentes para proporcionar orientación específica adicional para mejorar la resiliencia cibernética. La estrategia de seguridad cibernética, los informes de incidentes cibernéticos, el intercambio de inteligencia de amenazas y las pruebas de resiliencia cibernética siguen siendo el enfoque principal de las regulaciones más nuevas. La gestión de los riesgos cibernéticos que podrían surgir de las conexiones con proveedores de servicios externos se ha convertido en un elemento clave del marco de seguridad cibernética de "segunda generación". Además, ahora existen requisitos reglamentarios más específicos sobre la respuesta y recuperación de incidentes cibernéticos, así como sobre los informes de incidentes y los marcos de prueba de resiliencia cibernética. Además, en algunas jurisdicciones se han introducido requisitos regulatorios o expectativas relacionadas con cuestiones como las métricas de resiliencia cibernética y la disponibilidad de experiencia adecuada en seguridad cibernética en los bancos.

Las autoridades de las EMED tienden a ser más prescriptivas en sus regulaciones cibernéticas. La estrategia de ciberseguridad, los acuerdos de gobernanza, incluidos los roles y responsabilidades, y la naturaleza y frecuencia de las pruebas de resiliencia cibernética son algunas de las áreas en las que las autoridades de EMED proporcionan requisitos prescriptivos. Este enfoque parece estar relacionado con la necesidad de fortalecer la cultura de resiliencia cibernética en todo el sector financiero, las limitaciones de recursos y / o la falta de suficiente experiencia en seguridad cibernética en estas jurisdicciones. Por lo tanto, las autoridades de EMED pueden ver la necesidad de ser más claras en sus expectativas para asegurarse de que los consejos de administración y la alta dirección de los bancos inviertan en ciberseguridad y que el personal de los bancos sepa exactamente lo que deben hacer.

El trabajo internacional ha dado lugar a una convergencia en las regulaciones y expectativas de resiliencia cibernética en el sector financiero, pero se podría hacer más en algunas áreas. El trabajo del Grupo de Expertos Cibernéticos (CEG) del G7 y los organismos mundiales de normalización (SSB) sobre resiliencia cibernética ha facilitado la coherencia en las expectativas de regulación y supervisión financiera en todas las jurisdicciones. Esto es necesario dada la naturaleza sin fronteras del delito cibernético y su impacto potencial en la estabilidad financiera mundial. Otra área en la que podría haber margen para la convergencia es la forma en que las autoridades evalúan la ciber resiliencia de las instituciones supervisadas. Esto podría, por ejemplo, incluir alinear la evaluación de la adecuación de la gobernanza de seguridad cibernética, la fuerza laboral y las métricas de resiliencia cibernética de una empresa. Por último, podría haber margen para considerar un marco internacional para los proveedores externos críticos, en particular los proveedores de servicios en la nube, dado el posible impacto transfronterizo de un incidente cibernético en uno de estos proveedores.

Sección 1 – Introducción

1. El riesgo cibernético es una amenaza significativa para la estabilidad del sistema financiero y la economía global. El sistema financiero realiza una serie de actividades clave que apoyan la economía real (por ejemplo, toma de depósitos y préstamos, pagos y servicios de liquidación). Se ha demostrado que los incidentes cibernéticos interrumpen estas actividades al afectar las tecnologías de la información y la comunicación (TIC) de las que dependen ampliamente las empresas financieras y los datos que procesan. Dentro del sector financiero, los bancos suelen tener los productos y servicios más orientados al público. Sus múltiples puntos de contacto con partes externas dan lugar a vulnerabilidades significativas a los ataques cibernéticos y podrían usarse como puntos de entrada para ataques que pueden culminar en interrupciones relevantes para el sistema financiero.

2. El panorama de las amenazas cibernéticas sigue evolucionando y volviéndose más complejo en medio de la digitalización continua, el aumento de las dependencias de terceros y las tensiones geopolíticas. Interpol (2022) informa que el ransomware, el phishing, las estafas en línea y la piratería informática son las mayores amenazas de ciberdelincuencia a nivel mundial. Además, la complejidad del panorama de las amenazas cibernéticas ha aumentado debido al fuerte impacto de la geopolítica en las operaciones cibernéticas, especialmente desde que comenzó la guerra entre Rusia y Ucrania, con la denegación de servicio distribuida (DDoS) utilizada como una herramienta de guerra cibernética. También hay un resurgimiento del hacktivismo con una mayor sofisticación técnica y apoyo estatal, así como un aumento. Con respecto a la creciente dependencia de grandes partes del sistema financiero de los proveedores de la nube, CrowdStrike (2023) informa "una tendencia más amplia de delitos electrónicos y actores de estados-nación que adoptan el conocimiento y el oficio para explotar cada vez más los entornos de nube".

3. El panorama de las ciber amenazas también se caracteriza por un aumento significativo y continuo del coste de los ciber incidentes. Statista (2023) estimó el costo global del delito cibernético en 2022 en $ 8.4 billones y espera que esto supere los $ 11 billones en 2023. Esto refleja un aumento anual del 30% en el costo del delito cibernético durante el período 2021-23. Además, el costo promedio de una violación de datos entre 2020 y 2022 aumentó en un 13%, y la industria financiera obtuvo el segundo costo promedio más alto después de la atención médica con $ 6 millones.8 Según Chainalysis (2022), 2022 fue el año más grande para la piratería criptográfica, con $ 3.8 mil millones robados de negocios de criptomonedas. La demanda de seguros cibernéticos sigue superando la oferta y la brecha de protección cibernética parece estar ampliándose en medio de un mercado caracterizado por el aumento de las primas, la reducción de la cobertura y los estándares de suscripción más estrictos.

4. A la luz de los desarrollos anteriores, no es sorprendente que la resiliencia cibernética10 siga siendo una prioridad para la industria de servicios financieros. Según EY-IIF (2023), la mayoría de los directores de riesgos (CRO) consideran que el riesgo cibernético es la principal amenaza para la industria bancaria y "la más probable que resulte en una crisis o una interrupción operativa importante". A pesar de los importantes recursos invertidos en mejorar la resiliencia cibernética, las CRO destacan dos desafíos principales relacionados con la gestión efectiva del riesgo cibernético: (i) su presencia inherente en cada línea de negocio, en las operaciones diarias y en extensas redes de socios, proveedores y proveedores de servicios de los que los bancos dependen cada vez más; y ii) la creciente sofisticación de las herramientas y técnicas de piratería. Como resultado, los CRO esperan prestar la mayor atención al riesgo cibernético en los próximos 12 meses y considerarlo el principal riesgo estratégico para los próximos tres años. Una aspiración más general destacada por la industria es diseñar regulaciones más consistentes y coordinadas entre jurisdicciones de una manera que mejore la resiliencia cibernética global y reduzca la fragmentación regulatoria.

5. El fortalecimiento de la ciberresiliencia también es un enfoque clave para el sector oficial, incluidos los bancos centrales y las autoridades supervisoras. El delito cibernético se considera en general como una prioridad de defensa nacional y varias jurisdicciones han establecido políticas o marcos nacionales para fortalecer la ciberseguridad de sectores e instituciones críticos. Desde la perspectiva de la propia gestión del riesgo cibernético por parte de los bancos centrales, muchos han aumentado notablemente sus inversiones relacionadas con la seguridad cibernética desde 2020, dando prioridad al control técnico de seguridad y la resiliencia. y están colaborando dentro del marco proporcionado por el Centro de Coordinación de Resiliencia Cibernética (CRCC) del BIS. Además, la comunidad de bancos centrales está desarrollando marcos analíticos para comprender los canales a través de los cuales el riesgo cibernético puede crecer de una interrupción operativa a un evento sistémico. Por último, un número cada vez mayor de jurisdicciones han publicado directrices ciber específicas para el sector financiero y la ciberresiliencia ocupa un lugar destacado en los programas de trabajo de los organismos mundiales de normalización (SSB) y otros organismos internacionales.

6. La seguridad cibernética se considera una prioridad para los supervisores bancarios de todo el mundo. Dentro del sector financiero, las autoridades bancarias han sido particularmente activas en la elaboración de marcos regulatorios y de supervisión para mejorar la resistencia del sector bancario a los ataques cibernéticos. Esto refleja el hecho de que la ciberseguridad ocupa un lugar destacado en el programa de trabajo de los supervisores bancarios tanto de las economías avanzadas como de los mercados emergentes y en desarrollo (EMED). Este gráfico también sugiere que la máxima prioridad asignada a la ciberseguridad y la resiliencia operativa en general está correlacionada con el trabajo de supervisión sobre la digitalización del sistema financiero y su impacto en los modelos de negocio bancarios. En Europa, por ejemplo, la Supervisión Bancaria del BCE publicó sus prioridades supervisoras para 2023-25 en diciembre de 2022, que incluyen abordar las deficiencias en los marcos de resiliencia operativa, a saber, la externalización de TI y los riesgos de seguridad de TI/ciberseguridad.



7. Este documento actualiza Crisanto y Prenio (2017) revisando las regulaciones de seguridad cibernética en las jurisdicciones cubiertas en ese documento, así como examinando las emitidas en otras jurisdicciones. Además de las regulaciones de seguridad cibernética en la RAE de Hong Kong, Singapur, el Reino Unido y los Estados Unidos, que el documento de 2017 también cubrió, este documento examina las regulaciones cibernéticas en Australia, Brasil, la Unión Europea, Israel, Kenia, México, Perú, Filipinas, Ruanda, Arabia Saudita y Sudáfrica. Las jurisdicciones fueron elegidas para reflejar las regulaciones cibernéticas tanto en AE como en EMED. Esto pone de relieve el hecho de que, desde 2017, varias jurisdicciones, incluidas las EMED, han establecido o mejorado las regulaciones cibernéticas. Cabe señalar, sin embargo, que, según una encuesta del FMI realizada a 51 EMED, el 42% todavía carece de una regulación específica de ciberseguridad o gestión de riesgos tecnológicos.17 La Sección 2 proporciona el contexto internacional en el que estas regulaciones han evolucionado. La Sección 3 describe los diferentes enfoques en el diseño de regulaciones cibernéticas. La Sección 4 presenta los requisitos clave de la ciber regulación. La sección 5 concluye.

Sección 2 – Iniciativas regulatorias internacionales

8. La ciberresiliencia ocupa un lugar destacado en el programa de trabajo de las SSB. Dada la naturaleza sin fronteras de la ciberdelincuencia y su posible impacto en la estabilidad financiera mundial, la ciberresiliencia requiere cooperación internacional18 y, por lo tanto, ha ocupado un lugar destacado en el programa de trabajo de los organismos de seguridad financiera, incluidos el Consejo de Estabilidad Financiera (CEF), el Comité de Supervisión Bancaria de Basilea (CSBB), el Comité de Pagos e Infraestructuras del Mercado (CPMI), la Asociación Internacional de Supervisores de Seguros (IAIS) y la Organización Internacional de Valores Comisiones (OICV). Este trabajo tiene como objetivo lograr una mayor convergencia de los enfoques de resiliencia cibernética, principalmente a través de orientación basada en principios y herramientas prácticas. La convergencia se ha visto facilitada por el uso de un lenguaje común a través del léxico cibernético del FSB, que se publicó en 2018 y se actualizó en 2023.

9. El Grupo de Expertos Cibernéticos del G7 (G7 CEG) también desempeña un papel importante en la mejora de las prácticas de ciberresiliencia en el sector financiero. El G7 CEG se creó en 2015 para identificar los principales riesgos de seguridad cibernética en el sector financiero y proponer acciones que se tomarán en esta área en todas las jurisdicciones del G7, incluida la coordinación de políticas de seguridad cibernética. Las recomendaciones del G7 CEG tienen como objetivo reflejar los enfoques de políticas, la orientación de la industria y las mejores prácticas vigentes en todas sus jurisdicciones miembros. Si bien su enfoque principal está en las entidades financieras del sector privado, pueden ser de ayuda para el propio trabajo institucional de las autoridades financieras sobre la resiliencia cibernética y sus esfuerzos para promover esta resiliencia en todo el sector financiero. Dicho esto, las recomendaciones del G7 CEG no son vinculantes, no son prescriptivas y están diseñadas para adaptarse a los perfiles de riesgo individuales y los paisajes de amenazas, así como a los marcos legales y regulatorios específicos de cada país. El gráfico 2 ofrece un resumen de los principales trabajos de SSB y G7 CEG que están ayudando a facilitar la convergencia internacional de las regulaciones cibernéticas en el sistema financiero.

10. En general, los organismos de seguridad especial hacen hincapié en la importancia de la ciber resiliencia como parte de sus esfuerzos por mejorar la resiliencia operativa del sector financiero. El espectacular crecimiento de las amenazas relacionadas con la tecnología y la pandemia de Covid-19 pusieron de relieve la necesidad de mejorar la capacidad de las instituciones financieras para hacer frente a los eventos relacionados con el riesgo operativo que podrían causar interrupciones significativas en los mercados financieros, incluidos los incidentes cibernéticos. Con este objetivo, el CSBB publicó los Principios para la resiliencia operativa en 202120 para facilitar la capacidad de los bancos para resistir, adaptarse y recuperarse de esos eventos adversos graves. Un elemento clave de los Principios es garantizar un marco de TIC resiliente, incluida la ciberseguridad, para apoyar y facilitar plenamente la entrega de las operaciones críticas del banco. El boletín de BCBS 2021 sobre ciberseguridad no solo destaca la interacción entre la resiliencia operativa y la seguridad cibernética, sino también la necesidad de alinear la gestión del riesgo cibernético con los estándares ampliamente aceptados de la industria.

11. La Guía CPMI-OICV sobre ciber resiliencia para infraestructuras de los mercados financieros (FMI) se ha convertido en un punto de referencia clave para el sector financiero a la hora de diseñar un marco sólido para abordar el riesgo cibernético. Esta guía cibernética se publicó en 2016 con el propósito de complementar los Principios para FMI de 2012. Como tal, establece detalles adicionales relacionados con los preparativos y medidas que las FMI deben emprender para mejorar sus capacidades de resiliencia cibernética. La guía cibernética se centra en cinco categorías de gestión de riesgos cibernéticos: gobernanza; identificación; protección; detección; y respuesta y recuperación. También prevé tres componentes generales que se abordarán en todo el marco de la ciber resiliencia: pruebas; conciencia situacional; y aprender y evolucionar. Más recientemente, CPMI e IOSCO han centrado su atención en evaluar el nivel de adopción de sus orientaciones por parte de las infraestructuras del mercado financiero y los resultados han puesto de relieve los desafíos relacionados con el desarrollo de planes adecuados de respuesta y recuperación para hacer frente a incidentes cibernéticos graves.

12. Los elementos fundamentales de la ciberseguridad del G7 CEG son otro punto de referencia común para desarrollar e implementar un marco sólido de ciberresiliencia. Esta guía de 2016 ha desempeñado un papel fundamental al proporcionar a las instituciones y autoridades financieras los componentes básicos para diseñar e implementar políticas y prácticas sólidas de seguridad cibernética. Estos incluyen ocho elementos fundamentales que se basan en una estrategia y un marco de seguridad cibernética adecuados; una estructura de gobernanza eficaz; evaluación exhaustiva de los riesgos cibernéticos y los controles respectivos en todo el negocio; monitoreo sistemático de procesos para detectar rápidamente incidentes cibernéticos (por ejemplo, pruebas y auditorías); respuesta y recuperación oportunas ante incidentes; el intercambio oportuno de información pertinente; y la actualización periódica de los elementos fundamentales en consonancia con la evolución del panorama de amenazas. Para evaluar la eficacia con la que se están implementando estos elementos, el G7 CEG emitió herramientas en 2017 que describen los resultados y componentes deseables para evaluar el progreso en la mejora de la seguridad cibernética.

13. Con respecto a los componentes específicos de la resiliencia cibernética, el trabajo del FSB se ha centrado en la respuesta y recuperación de incidentes cibernéticos, así como en la notificación de incidentes cibernéticos. En 2020, el FSB emitió un informe final que proporciona un conjunto de herramientas para guiar la respuesta de las instituciones financieras y la recuperación de un incidente cibernético de una manera que limite los riesgos relacionados con la estabilidad financiera. Dado que esto requiere información oportuna y precisa sobre incidentes cibernéticos, el FSB emitió recomendaciones en 2023 para abordar los impedimentos para lograr una mayor convergencia en la notificación de incidentes cibernéticos, incluida la propuesta de un concepto para un formato común para el intercambio de informes de incidentes (FIRE) para abordar los desafíos operativos derivados de la presentación de informes a múltiples autoridades y fomentar una mejor comunicación.

14. El G7 CEG ha proporcionado orientación adicional para evaluar la eficacia de las medidas de ciber resiliencia y abordar las amenazas de ransomware. En 2018, el G7 CEG elaboró aún más sus elementos fundamentales de seguridad cibernética al proporcionar a las empresas del sector financiero una guía para evaluar su resistencia a incidentes cibernéticos maliciosos a través de la simulación y una guía para las autoridades del sector financiero que consideran el uso de pruebas de penetración dirigidas por amenazas (TLPT) dentro de sus jurisdicciones. Además, reconociendo la necesidad de procedimientos de respuesta y recuperación claramente definidos y ensayados regularmente en caso de eventos cibernéticos disruptivos, el G-7 CEG desarrolló herramientas en 2020 para guiar el establecimiento de programas de ejercicios cibernéticos con partes interesadas internas y externas. Estas herramientas también podrían servir como guía para establecer programas de ejercicios cibernéticos en todas las jurisdicciones y sectores. Además, para hacer frente al reciente crecimiento de la amenaza de ransomware en el sector financiero, el G7 CEG emitió consideraciones clave en 2022 que son esenciales para abordar esta amenaza.

15. La mejora de la gestión de riesgos cibernéticos por terceros también ha formado parte del programa de trabajo del CEG y el CEB del G7. El uso de terceros generalmente introduce riesgos cibernéticos adicionales que deben gestionarse bien. En 2018, el CEG del G7 emitió los elementos fundamentales que debían tenerse en cuenta a lo largo del ciclo de vida de la gestión del riesgo cibernético de terceros, no solo dentro de una entidad individual, sino también como parte del monitoreo del riesgo cibernético en todo el sistema, incluso con fines de coordinación intersectorial. En 2022, el G7 CEG revisó estos elementos fundamentales para reflejar los últimos desarrollos de la industria financiera, en particular la mayor dependencia de los proveedores de TIC y la necesidad de gestionar eficazmente las exposiciones cibernéticas relacionadas con la cadena de suministro de TIC. Complementando este trabajo, el programa de trabajo del FSB para 2023 incluye la publicación de un documento consultivo destinado a fortalecer la capacidad de las instituciones financieras para gestionar el riesgo de terceros y externalización.

16. El IAIS (2023) informa que el seguro cibernético solo cubre una pequeña proporción del costo económico potencial resultante de los eventos cibernéticos. Las aseguradoras no solo están expuestas a riesgos cibernéticos en sus operaciones, sino que también son tomadores activos del riesgo cibernético a través de sus actividades de suscripción cibernética. Con respecto a esto último, el Informe de Suscripción de Riesgos Cibernéticos de IAIS 2020 concluyó que las prácticas de suscripción cibernética, aunque útiles, aún no eran óptimas, particularmente debido a los desafíos que rodean la medición de las exposiciones al riesgo y la claridad de las pólizas de seguro cibernético. En vista de ello, el informe recomendó una atención proactiva de supervisión para facilitar el seguimiento, la comprensión y la evaluación de la exposición y el impacto de la suscripción de riesgos cibernéticos; así como mejorar la experiencia supervisora correspondiente.

17. En términos más generales, las SSB han dedicado recursos para aumentar la comprensión mutua de sus miembros de sus esfuerzos individuales para fortalecer la ciber resiliencia. Esto ha tomado principalmente la forma de un inventario de las regulaciones, orientación y prácticas de supervisión de seguridad cibernética. Ejemplos de este trabajo son el informe del FSB de 2017 Stocktake of Public Released Cybersecurity Regulations, Guidance and Supervisory Practices, que se realizó con las jurisdicciones miembros del FSB, y el informe de BCBS de 2018 titulado Cyberresilience: range of practices, que describe y compara el rango de prácticas de ciber resiliencia regulatoria y supervisora en todas las jurisdicciones miembros de BCBS. Otro ejemplo relevante es el informe de 2019 del Grupo de Trabajo Cibernético de IOSCO. Este informe examina cómo las jurisdicciones miembros de la OICV están utilizando marcos cibernéticos reconocidos internacionalmente y cómo estos marcos podrían ayudar a abordar cualquier brecha identificada en los regímenes actuales de los miembros de la OICV en lugar de proponer nuevas orientaciones.



Sección 3 – Diseño de regulaciones de resiliencia cibernética

18. Hay dos enfoques predominantes para la regulación de la resiliencia cibernética de los bancos: el primero aprovecha las regulaciones relacionadas existentes y el segundo implica la emisión de regulaciones cibernéticas integrales. En el primer enfoque, las regulaciones relacionadas existentes (por ejemplo, regulaciones sobre gestión de riesgos operativos, gestión de riesgos de TI, subcontratación) se mejoran para incluir elementos específicos de la cibernética. Este enfoque considera el riesgo cibernético como cualquier otro riesgo y, por lo tanto, también se aplican los requisitos generales para la gestión de riesgos (por ejemplo, gobernanza, establecimiento del apetito de riesgo) y los requisitos sobre TI, seguridad de la información y riesgos operativos. Como resultado, este enfoque facilita una fuerte alineación con las expectativas regulatorias sobre la gestión del riesgo empresarial y el riesgo operativo, incluida la resiliencia operativa. Este enfoque se observa más comúnmente en jurisdicciones (por ejemplo, Estados Unidos y Europa) que ya han establecido regulaciones sobre gestión de riesgos operativos, continuidad del negocio, seguridad de la información y / o gestión de riesgos de tecnología de la información. El segundo enfoque, por otro lado, busca cubrir todos los aspectos de la ciberseguridad, desde los acuerdos de gobernanza hasta los procedimientos operativos, en una regulación integral. Este es el caso, por ejemplo, de México y de la consulta pública de Sudáfrica sobre la Norma Conjunta sobre Requisitos de Ciberseguridad y Ciber resiliencia.

19. En cualquiera de los dos enfoques, existe el riesgo de que los reglamentos se vuelvan demasiado prescriptivos o den lugar a ineficiencias. Existe el riesgo de que la regulación se vuelva demasiado prescriptiva, por lo que se queda atrás tanto de la amenaza en constante evolución del riesgo cibernético como de los avances en la gestión del riesgo cibernético. También existe el riesgo de crear ineficiencias y silos. Las regulaciones cibernéticas integrales, en particular, podrían dar lugar a que las instituciones financieras establezcan marcos de gobernanza y gestión de riesgos para el riesgo cibernético y la resiliencia que estén separados de sus marcos para toda la empresa.

20. Para contrarrestar el riesgo de demasiada prescripción, está surgiendo un enfoque regulador que busca combinar principios amplios de ciberresiliencia con un conjunto de requisitos básicos. Este enfoque se centra más en "qué expectativas lograr" y menos en "cómo alcanzarlas".25 Apoya un marco regulatorio que sea lo suficientemente flexible como para adaptarse a la naturaleza dinámica y evolutiva del riesgo cibernético, al tiempo que tiene expectativas claras de supervisión con respecto a los aspectos centrales de la gobernanza y la gestión de riesgos que apuntan a mejorar la resiliencia cibernética. Por ejemplo, la Autoridad Australiana de Regulación Prudencial (APRA) publicó la Guía de Prácticas Prudenciales CPG 234 Seguridad de la Información, que proporciona expectativas detalladas con respecto a los requisitos establecidos en la Norma Prudencial CPS 234 – Seguridad de la Información.

21. Encontrar el nivel correcto de prescripción al desarrollar regulaciones de resiliencia cibernética es un desafío. Si bien las normas prescriptivas pueden ser necesarias en algunas áreas, por ejemplo, al exigir a los consejos de administración de los bancos que establezcan un marco de gestión del riesgo cibernético y el apetito de riesgo, otras áreas son claramente menos adecuadas para reglas específicas y es importante evitar que las regulaciones se queden atrás tanto de la amenaza en constante evolución del riesgo cibernético como de los avances en la gestión del riesgo cibernético. Por ejemplo, dada la tasa de cambio tecnológico, es probable que cualquier regulación que prescriba el uso de una tecnología específica se vuelva rápidamente obsoleta e ineficaz.26 Exigir un tiempo de recuperación específico es otro ejemplo en el que los reguladores deben tener cuidado con la forma en que los bancos la implementan. El objetivo es evitar la interrupción prolongada de las operaciones financieras críticas, pero un tiempo de recuperación excesivamente estricto y rígido puede resultar contraproducente si esto se produce a expensas de la capacidad de los bancos para verificar minuciosamente que todos sus sistemas ya no están comprometidos. Las regulaciones que son muy prescriptivas también pueden resultar en un enfoque basado en el cumplimiento para lidiar con el riesgo cibernético.

22. Ya sea como parte de regulaciones relacionadas o integrales separadas, también se puede hacer una distinción entre regulaciones cibernéticas "más antiguas" (primera generación) y "más nuevas" (segunda generación). Las autoridades reconocen que la gestión del riesgo cibernético está en constante evolución. Por lo tanto, el enfoque de la primera generación y la segunda generación de regulaciones cibernéticas son algo diferentes. La primera generación se centró en establecer un enfoque de gestión de riesgos cibernéticos y definir requisitos sobre controles de seguridad típicos (por ejemplo, controles de acceso y análisis de vulnerabilidades). La segunda generación va un paso más allá, enfatizando la necesidad de desarrollar capacidades (por ejemplo, gestión de incidentes cibernéticos, informes de incidentes cibernéticos y gestión de riesgos de terceros) esenciales para garantizar la resiliencia cibernética de una institución financiera en un sistema financiero cada vez más digital. Las autoridades también están pensando continuamente en formas de mejorar sus regulaciones cibernéticas. Podrían, por ejemplo, centrarse en el establecimiento de acuerdos de continuidad de las actividades que impliquen la coordinación entre las instituciones financieras pertinentes para responder a las crisis sistémicas causadas por incidentes cibernéticos.

23. Independientemente del enfoque regulador adoptado, la aplicación del principio de proporcionalidad se tiene debidamente en cuenta en la aplicación de los marcos de ciberresiliencia. La proporcionalidad se define como la aplicación de normas prudenciales simplificadas a bancos más pequeños y menos complejos para evitar costes de cumplimiento excesivos sin socavar las salvaguardias prudenciales clave.27 Trasladar este concepto al mundo de la ciberseguridad es un desafío, dado que la exposición al riesgo cibernético depende no solo del tamaño y la complejidad de un banco, sino también de cómo utiliza la tecnología y cómo proporciona sus productos y servicios utilizando canales digitales. así como el nivel de interconexión del sector financiero. Las autoridades tienen como objetivo identificar aspectos clave de la gobernanza de la resiliencia cibernética y la gestión de riesgos que deberían aplicarse a todas las empresas supervisadas, independientemente de los indicadores tradicionales utilizados para agrupar a los bancos pares. Al mismo tiempo, otras autoridades, como la Superintendencia de Bancos y Fondos de Pensiones Privados de Perú, aplican un marco de proporcionalidad en el que los bancos sistémicamente importantes están sujetos a mayores requisitos de resiliencia cibernética que reflejan sus posibles riesgos para la estabilidad financiera.

24. Las evaluaciones de supervisión de las capacidades de ciberseguridad tienden a utilizar las normas técnicas existentes para la seguridad cibernética y de la información como un valioso punto de referencia. Las jurisdicciones tienen en cuenta los estándares de la industria al desarrollar sus marcos regulatorios y de supervisión. Las normas técnicas creíbles proporcionan conocimientos esenciales de prácticas y controles para gestionar los riesgos cibernéticos y tecnológicos. Ejemplos de estándares técnicos influyentes en la comunidad de seguridad cibernética / de la información incluyen:

• el marco de seguridad cibernética del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos;

• las normas de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI), en particular la serie ISO/IEC 27000 sobre gestión de la seguridad de la información, ISO 22301 sobre seguridad y resiliencia e ISO 31000 sobre gestión de riesgos;

• Marco de objetivos de control de ISACA para tecnologías de la información (COBIT) para el gobierno y la gestión de TI; y

• El Centro de Controles de Seguridad de Internet (CIS).



Sección 4 – Requisitos reglamentarios clave para la ciberresiliencia

25. Como se mencionó en la Sección 3, los reguladores en diferentes jurisdicciones tienen dos formas amplias de comunicar sus requisitos o expectativas de seguridad cibernética. Algunos reguladores emiten regulaciones "todo en uno" que abarcan todos los aspectos de la seguridad cibernética. Otros reguladores insertan requisitos de seguridad cibernética en varias regulaciones relevantes (por ejemplo, relacionadas con TI, proveedores de servicios externos). En ambos casos, las regulaciones comparten un alto grado de similitud, lo que se espera dado que se basan en estándares regulatorios y de la industria internacionales. Esta sección analiza los requisitos y expectativas regulatorios clave, ya sea que se encuentren en regulaciones "todo en uno" o insertadas en regulaciones relevantes, en las áreas de estrategia y gobierno de seguridad cibernética; respuesta y recuperación de incidentes cibernéticos; informes de incidentes cibernéticos e intercambio de inteligencia de amenazas; pruebas de resiliencia cibernética; ciber higiene; dependencias de terceros; cultura y concienciación sobre la ciberseguridad; fuerza laboral de seguridad cibernética; y métricas de resiliencia cibernética.

Estrategia y gobernanza de la ciberseguridad

26. Un número cada vez mayor de reguladores, en particular en las EMED, exigen a los bancos que desarrollen "estrategias" específicas de ciberseguridad.28 Sin embargo, es posible que las reglamentaciones no las llamen explícitamente estrategias, sino que se refieran a ellas como "políticas", "programas" o "marcos". Dichos requisitos reglamentarios suelen seguir el marco de ciberseguridad defendido en CPMI-IOSCO (2016) que implica identificación, protección, detección, respuesta y recuperación (véase el gráfico 2). Más concretamente, esas estrategias, políticas, programas y marcos incluyen los siguientes elementos básicos:

• mapeo de la exposición al riesgo cibernético;

• definir planes de acción para abordar los riesgos cibernéticos mapeados;

• asignar recursos para aplicar planes de acción;

• definir y asignar funciones y responsabilidades;

• revisión continua de la adecuación de los controles;

• seguimiento del panorama de amenazas;

• reportar a la junta y a la alta gerencia; y

• promover la conciencia y la cultura de ciberseguridad.



27. Los mismos reguladores que requieren estrategias específicas de ciberseguridad también especifican acuerdos de gobernanza de la ciberseguridad. Tales acuerdos de gobernanza requieren que la junta establezca y apruebe la estrategia, el marco y la política de seguridad cibernética del banco, y supervise su implementación por parte de la alta gerencia. Por otro lado, se requiere que la alta gerencia desarrolle el marco y la política de seguridad cibernética del banco en línea con la estrategia general, implemente el marco y la política y supervise su efectividad. Otras regulaciones, particularmente aquellas en AE, generalmente no especifican acuerdos de gobernanza de seguridad cibernética. Presumiblemente, estas regulaciones consideran que los marcos generales de gestión de riesgos existentes, particularmente aquellos para la seguridad de la información o el riesgo / resiliencia operacional, ya cubren las funciones y responsabilidades de la junta y la alta gerencia cuando se trata de abordar los riesgos cibernéticos.

28. La orientación reglamentaria y los requisitos relacionados con las funciones y responsabilidades de la ciberseguridad son comunes. Si bien la mayoría de los reguladores no requieren que los bancos implementen el modelo de gestión de riesgos de "tres líneas de defensa", las regulaciones a menudo requieren políticas documentadas sobre la asignación clara de responsabilidades de gestión relacionadas con el ciberespacio relacionadas con la identificación, protección, detección y respuesta y recuperación. Se enfatizan los roles de la junta y la alta dirección. En algunos casos, la orientación o los requisitos regulatorios incluyen la designación de una unidad, función o posición que es responsable de la implementación de la seguridad cibernética dentro del banco.

29. La designación de una persona responsable de la ciberseguridad al más alto nivel es cada vez más obligatoria. La posición exacta puede no estar especificada en las regulaciones, pero es común que esta posición se requiera para ser una posición de nivel C (es decir, parte de la alta dirección). Al dar prominencia a esta posición, también parece haber un impulso para resaltar que la ciberseguridad ya no es solo un área de gestión de riesgos y continuidad del negocio de TI, sino una parte explícita de la gestión de riesgos empresariales de un banco. El requisito de designar un director de seguridad de la información (CISO) o equivalente parece ser más común en las EMED (por ejemplo, Brasil, Kenia, México, Filipinas y Arabia Saudita), pero también es posible encontrar ejemplos en EA como el UK29. Sin embargo, la falta de profesionales de seguridad de la información en estas jurisdicciones podría plantear desafíos para la implementación de este requisito. Este problema no es exclusivo de las EMED. De hecho, los requisitos de seguridad cibernética del Departamento de Servicios Financieros del Estado de Nueva York (DFSNY) para las empresas de servicios financieros, por ejemplo, permiten que el CISO sea empleado por un proveedor de servicios externo del banco (es decir, no un empleado), sujeto a ciertas condiciones. Presumiblemente, esto es para anticipar el desafío que las instituciones más pequeñas podrían enfrentar al contratar CISO.

30. En general, los reguladores esperan que los bancos puedan identificar sus operaciones críticas30, incluidos los activos de información de apoyo. A nivel nacional, los gobiernos identifican la infraestructura crítica y las empresas a las que se aplican sus marcos nacionales de seguridad cibernética. Se espera que los bancos hagan lo mismo a su propio nivel. Los bancos deben poder asignar sus operaciones a sus activos de apoyo y poder clasificar sus operaciones de acuerdo con su criticidad y sensibilidad al riesgo cibernético. Esto permite centrar los esfuerzos de seguridad cibernética en operaciones y activos de información críticos y sensibles desde el punto de vista operativo. Idealmente, todo el banco debería estar protegido, pero, dados los recursos limitados, los bancos deberían poder desplegar sus recursos de manera específica para maximizar los beneficios y garantizar la resiliencia operativa.

Respuesta y recuperación de incidentes cibernéticos

31. La gestión de incidentes cibernéticos es sin duda uno de los pilares de un marco sólido de ciberresiliencia. La gestión de incidentes es un proceso de TI típico y bien establecido. Pero la complejidad y el alto impacto de los incidentes cibernéticos han llevado a casi todas las jurisdicciones consideradas en el análisis a reforzar las disposiciones de sus regulaciones que especifican que los bancos deben establecer procesos y capacidades para gestionar adecuadamente los incidentes cibernéticos. Un banco debe ser capaz de gestionar los incidentes cibernéticos a lo largo de su ciclo de vida. Esto debería incluir el establecimiento de criterios de clasificación y procedimientos de escalamiento y presentación de informes. Algunas jurisdicciones estipulan que los bancos también deben considerar los incidentes que ocurrieron en proveedores externos en su marco de gestión de incidentes cibernéticos.

32. Muchos reguladores exigen ahora a los bancos que elaboren planes de respuesta y recuperación de incidentes cibernéticos (CIRR), además del requisito general de gestión de incidentes. Teniendo en cuenta que se trata de cuándo, no de si, los bancos experimentarán un ataque cibernético, ahora se requiere generalmente que las instituciones supervisadas tengan planes de respuesta y recuperación que les permitan responder rápidamente a un incidente cibernético, mitigando su impacto y facilitando la rápida recuperación de las operaciones del banco.31 Esta mentalidad de "asumir incumplimiento" ha reemplazado totalmente el concepto tradicional de construir un perímetro fuerte para evitar un ataque cibernético. El nuevo entorno de amenazas, caracterizado por múltiples puntos de entrada potenciales para los ataques, ha reducido la eficacia del enfoque de seguridad tradicional, que se basa únicamente en la organización de todos los dispositivos de seguridad / capacidad de detective de una institución para proteger el perímetro. El enfoque de supuesto de violación complementa las medidas tradicionales con técnicas de detección de intrusos, así como medidas de respuesta (por ejemplo, para evitar la extracción de datos críticos). Las jurisdicciones que buscan fortalecer su marco de resiliencia cibernética mediante la introducción de requisitos CIRR están tomando cada vez más nota del kit de herramientas CIRR del FSB.

33. Los reguladores suelen subrayar que los planes del CIRR deben probarse y revisarse constantemente para garantizar una capacidad adecuada de respuesta y recuperación. Dada la dinámica y la creciente complejidad de los ataques cibernéticos, los reguladores esperan que los bancos evalúen periódicamente la idoneidad de sus planes CIRR para gestionar los incidentes cibernéticos. Las lecciones aprendidas de incidentes anteriores son esenciales para mejorar los planes de CIRR, permitiendo así a los bancos responder adecuadamente a los ataques cibernéticos. La prueba de los planes CIRR generalmente se requiere en las regulaciones de resiliencia cibernética, como se puede ver en el estándar prudencial de APRA sobre seguridad de la información y en el estándar conjunto propuesto sobre requisitos de ciberseguridad y resiliencia cibernética bajo consulta pública en Sudáfrica. En el caso de la norma propuesta en Sudáfrica, una institución financiera debe probar todos los elementos de su capacidad de resiliencia cibernética y controles de seguridad para determinar la efectividad general, si se implementa correctamente, opera según lo previsto y produce los resultados deseados. Además, hay varios ejemplos que muestran a las autoridades y/o asociaciones comerciales llevando a cabo ejercicios sectoriales para probar la capacidad de las instituciones financieras para responder y recuperarse de eventos disruptivos de manera coordinada.

34. La experiencia con los ciberataques demuestra la importancia de coordinar la gestión de incidentes cibernéticos, la gestión de crisis y la continuidad del negocio. Los ataques de ransomware exitosos son ejemplos de incidentes cibernéticos que pueden convertirse rápidamente en una crisis, dado el potencial de interrumpir completamente las operaciones de un banco. Las buenas prácticas bancarias muestran la utilidad de definir y revisar periódicamente los criterios que deben utilizarse para caracterizar las situaciones de crisis, permitiendo así que los procedimientos de gestión de crisis y continuidad del negocio se activen adecuadamente en caso de escalada de incidentes.

Informes de incidentes cibernéticos e intercambio de inteligencia de amenazas

35. La notificación de incidentes cibernéticos y el intercambio de inteligencia sobre amenazas son herramientas valiosas para aumentar el conocimiento situacional del panorama de las amenazas cibernéticas. Por un lado, la notificación de incidentes cibernéticos es importante para evaluar el impacto de los incidentes exitosos, así como para anticipar la probabilidad de que se materialice el riesgo sistémico (por ejemplo, las implicaciones sistémicas de una infección de ransomware en una infraestructura crítica del mercado financiero). Por otro lado, el intercambio de inteligencia de amenazas constituye una fuente importante de información sobre amenazas y vulnerabilidades, lo que permite a los bancos evaluar la idoneidad de sus controles de seguridad cibernética.

36. La comunicación oportuna de incidentes cibernéticos materiales es común en todas las regulaciones. Aunque los plazos y los umbrales de materialidad varían, muchos reguladores establecen requisitos para la notificación de incidentes cibernéticos, incluida la notificación de incidentes cibernéticos materiales lo antes posible, seguido de un informe completo en una fecha posterior. La notificación oportuna de un incidente importante permite a las autoridades comenzar a monitorear el impacto del incidente en bancos individuales y en el sistema financiero, mientras que el informe completo es útil para recopilar información de inteligencia de amenazas y un análisis de causa raíz que podría compartirse con los bancos o apoyar las actividades de supervisión. En algunos casos, es posible que se requieran informes intermedios para proporcionar información actualizada sobre la ocurrencia. Por ejemplo, la Autoridad Monetaria de Singapur (MAS) requiere que el incidente se informe dentro de una hora de que ocurra, y luego se presente un análisis de causa e impacto raíz a la autoridad dentro de los 14 días posteriores al descubrimiento del incidente.32 Sin embargo, al examinar una muestra más amplia de 51 EMED, el FMI encontró que el 54% carece de un régimen específico de notificación de incidentes cibernéticos.

37. Aunque los requisitos varían de una jurisdicción a otra, algunas autoridades han comenzado a desarrollar sus propias iniciativas de intercambio de inteligencia sobre amenazas. Los reguladores reconocen la relevancia del intercambio de información sobre cuestiones de seguridad para el desarrollo de un marco sólido de resiliencia cibernética. Aunque no existe un enfoque común para el intercambio de inteligencia sobre amenazas, este es uno de los elementos clave del marco de ciberresiliencia de algunas jurisdicciones, como Brasil34, la UE y Arabia Saudí. El intercambio de inteligencia sobre amenazas es una práctica que aún está madurando. Algunos reguladores están desarrollando sus propias iniciativas, como la iniciativa de intercambio de información e inteligencia cibernética del BCE (CIISI-EU). En Arabia Saudita, los principios de inteligencia de amenazas cibernéticas (CTI) describen las mejores prácticas centradas en producir, procesar y difundir inteligencia de amenazas para mejorar la identificación y mitigación de amenazas cibernéticas relevantes para el sector financiero a través de inteligencia de amenazas procesable. También hay iniciativas lideradas por la industria, como el Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC).

Pruebas de resiliencia cibernética

38. Los reguladores esperan que los bancos realicen pruebas de ciberresiliencia y aborden los problemas identificados. La Guía CPMI-IOSCO sobre resiliencia cibernética para infraestructuras de mercados financieros, que ha proporcionado un enfoque coherente para mejorar la resiliencia cibernética en las instituciones financieras en general, pidió el establecimiento de un marco integral de resiliencia cibernética que incluya un programa de prueba para validar la efectividad del marco. Ese programa de pruebas podría emplear diversas metodologías y prácticas de prueba, como la evaluación de la vulnerabilidad, las pruebas de penetración, las simulaciones de mesa y el TLPT.

39. En general, los reguladores bancarios no especifican la naturaleza y la frecuencia de las pruebas. Por lo general, estos dependen de una serie de factores, incluidos el tamaño y la complejidad de un banco, la criticidad y la sensibilidad de sus servicios comerciales y activos de información, y los cambios en el panorama de amenazas. Curiosamente, algunos reguladores en las EMED tienden a ser más prescriptivos. Los requisitos comunes en estas jurisdicciones incluyen pruebas de penetración anuales y evaluaciones de vulnerabilidad semestrales o escaneos sistemáticos de los sistemas de información de los bancos. Sin embargo, muchas EMED todavía no exigen pruebas y ejercicios cibernéticos ni proporcionan más orientación.

40. Se reconoce la importancia del TLPT. Varios reguladores de las economías desarrolladas cuentan con marcos TLPT, aunque los objetivos y los detalles de la implementación pueden diferir.36 Los marcos se aplican típicamente a instituciones financieras grandes o críticas, pero las autoridades pueden tener la discreción de incluir a otras instituciones financieras, como los bancos considerados riesgosos desde una perspectiva supervisora. Los marcos también difieren en términos de si los proveedores de inteligencia de amenazas y prueba de equipo rojo deben ser externos a la institución financiera, acreditados y evaluados formalmente.

41. Algunos reguladores coordinan o participan en ejercicios cibernéticos destinados a probar eventos de crisis que podrían perturbar el sistema financiero u otras infraestructuras nacionales críticas. Dada la mayor complejidad de los servicios financieros y la creciente interconexión entre las instituciones financieras, algunas jurisdicciones están aprovechando las capacidades de prueba de los bancos y otros actores relevantes mediante la introducción de escenarios y el desarrollo de planes para responder a las principales perturbaciones del sistema financiero (por ejemplo, la falta de disponibilidad de sistemas de pago críticos). Aunque no suelen estar cubiertas por actividades reguladoras o de supervisión, estas iniciativas contribuyen al desarrollo de controles y prácticas para mitigar posibles crisis sistémicas. Del mismo modo, vale la pena mencionar que algunos ejercicios cibernéticos nacionales involucran diferentes sectores que podrían verse afectados por incidentes cibernéticos disruptivos, como energía, telecomunicaciones y servicios financieros.

Ciber higiene

42. Dado que varios ciberataques exitosos son el resultado de deficiencias rutinarias en el mantenimiento básico y la seguridad del hardware y los programas informáticos, no es sorprendente que la higiene cibernética sea un elemento clave de las regulaciones cibernéticas de los bancos, así como en las estrategias nacionales de seguridad cibernética. Los reguladores han agregado requisitos de higiene cibernética a sus regímenes. Por ejemplo, en los Estados Unidos, las expectativas de supervisión para una postura efectiva de seguridad cibernética incluyen la higiene cibernética básica, como la gestión de activos de TI, la gestión de vulnerabilidades y la gestión de parches. En Singapur, los bancos (y otras instituciones financieras) deben cumplir con los requisitos de higiene cibernética relacionados con la seguridad de cuentas con privilegios completos y acceso sin restricciones; aplicar parches de seguridad periódicos; establecer normas de seguridad básicas; despliegue de dispositivos de seguridad de red; implementar medidas antimalware; y el fortalecimiento de la autenticación de usuarios.

Dependencias de terceros

43. Los bancos utilizan ampliamente terceros para proporcionar servicios, sistemas y soluciones informáticas que respaldan las operaciones de los bancos. Tradicionalmente, los terceros se refieren a los proveedores de actividades subcontratadas. En el contexto de la ciberseguridad, los terceros pueden definirse en un sentido mucho más amplio para incluir productos y servicios que normalmente no se consideran externalizados (por ejemplo, suministro de energía, líneas de telecomunicaciones, hardware, software), así como contrapartes interconectadas (por ejemplo, sistemas de pago y liquidación, plataformas de negociación, depositarios centrales de valores y contrapartes centrales). Estos terceros pueden tener o pueden acceder a información no pública de los bancos y sus clientes. Además, las vulnerabilidades de seguridad cibernética en estos terceros podrían convertirse en canales de ataque a los bancos. Las capacidades de seguridad de los proveedores de servicios externos son, por lo tanto, elementos críticos de cualquier marco de seguridad cibernética.

44. En la mayoría de los casos, los reguladores utilizan reglamentos de subcontratación para abordar las dependencias de terceros. Las reglamentaciones de externalización suelen exigir la notificación previa o la autorización de las actividades de externalización de materiales, el mantenimiento de un inventario de funciones subcontratadas y la presentación de informes sobre las mediciones de los acuerdos de nivel de servicio (SLA) y la realización adecuada de los controles. Algunas regulaciones de subcontratación también requieren que las actividades de subcontratación sean visibles para las entidades reguladas para que puedan gestionar los riesgos asociados. Además, las reglamentaciones de contratación externa generalmente requieren que los bancos desarrollen marcos contractuales y de contratación de contratación aprobados por la administración y/o la junta directiva que definan las políticas y la gobernanza de la subcontratación de los bancos y establezcan las obligaciones respectivas de la institución y el proveedor de servicios en un acuerdo de subcontratación.

45. Las regulaciones enfatizan la importancia de alinear la continuidad del negocio, así como la confidencialidad e integridad de la información cuando se trata de terceros. Los planes de continuidad del negocio de terceros proveedores críticos (y sus subcontratistas) deben estar alineados con las necesidades y políticas del banco en términos de continuidad del negocio y seguridad. La confidencialidad y la integridad de los datos se enfatizan especialmente cuando se trata de terceros que prestan servicios de procesamiento de datos. Este problema se aborda en los requisitos generales de protección de datos, los términos contractuales que deben incluir un acuerdo de confidencialidad y los requisitos de seguridad para salvaguardar los datos de un banco y sus clientes.

46. Muchas jurisdicciones tienen requisitos reglamentarios específicos para el uso de la nube por parte de los bancos. Estos van desde requerir que la información transferida a la nube esté sujeta a una cláusula contractual sobre confidencialidad y seguridad de datos hasta requisitos más específicos. Ejemplos de requisitos específicos incluyen aquellos relacionados con la ubicación de datos (por ejemplo, restringir la transferencia de datos al extranjero, el requisito de que la ubicación de al menos un centro de datos para servicios de computación en la nube esté en el país o región), segregación de datos, limitaciones de uso de datos (por ejemplo, requerir el consentimiento explícito del cliente para el manejo de datos por parte de terceros), tratamiento de datos en caso de una salida del acuerdo con terceros, y el derecho a auditar.

47. Más recientemente, al menos un par de jurisdicciones han avanzado hacia marcos de supervisión para terceros críticos. La creciente dependencia de las instituciones financieras de la tecnología y la complejidad e interconexiones adicionales que la tecnología ha aportado al ecosistema financiero plantean riesgos operativos no solo para las instituciones individuales sino también para el sistema financiero. Esto es especialmente cierto para el creciente uso de servicios en la nube, en el que la interrupción podría tener graves consecuencias para el sistema financiero nacional e internacional. Esto se debe en gran parte a que los servicios en la nube son proporcionados por solo un puñado de compañías de tecnología, que operan a nivel mundial. Esto pone de relieve que el enfoque actual de confiar en las instituciones financieras para gestionar los riesgos derivados de los servicios de terceros puede no ser suficiente, y que puede ser necesario complementarlo con un marco de supervisión para terceros críticos. La UE ya ha aprobado su Ley de Resiliencia Operativa Digital (DORA), que establece este marco de supervisión. En el Reino Unido, el Banco de Inglaterra y la Autoridad de Conducta Financiera (los reguladores del Reino Unido) publicaron conjuntamente un documento de debate sobre el mismo tema, tras la emisión de una declaración de política por parte del Tesoro del Reino Unido. Los comentarios sobre el documento de debate se incorporarán a un documento de consulta que se espera que se publique después de que se adopte la legislación primaria pertinente que otorga a los reguladores del Reino Unido la supervisión de terceros críticos (actualmente ante el Parlamento del Reino Unido). Estos se suman a las jurisdicciones que ya tienen poderes de inspección sobre terceros, ya sea a través de requisitos formales (por ejemplo, Singapur y los Estados Unidos) o compromisos voluntarios (por ejemplo, Australia).

Cultura y conciencia de seguridad cibernética

48. Los reguladores bancarios hacen hincapié en la importancia de difundir una cultura de ciberseguridad al personal de los bancos, los proveedores externos, los clientes y los usuarios. Los reguladores destacan la responsabilidad de la junta y la alta dirección de promover una cultura de seguridad cibernética, que generalmente está respaldada por programas de capacitación adecuados para diferentes audiencias objetivo (personal, proveedores, clientes, etc.). En los Estados Unidos, una institución supervisada con una sólida cultura de seguridad generalmente integra su programa de seguridad de la información en su línea de negocios, funciones de soporte, gestión de terceros y nuevas iniciativas. La regulación brasileña requiere que los bancos establezcan mecanismos para la difusión de una cultura de seguridad cibernética dentro de la institución, incluida la provisión de información a los clientes y usuarios sobre las precauciones al usar productos y servicios financieros.

49. La mayoría de los reguladores establecen requisitos de sensibilización y capacitación en materia de ciberseguridad. Según Ponemon Institute (2022), los empleados o contratistas negligentes son una fuente importante de incidentes de seguridad cibernética. A la luz de esto, la mayoría de las regulaciones requieren programas de concientización sobre seguridad cibernética para el personal, los contratistas y los proveedores de servicios de la institución supervisada. Estos programas tienen como objetivo reforzar la cultura de ciberseguridad de la institución. Por lo general, adoptan la forma de capacitación periódica y se prevé que cubran al menos el panorama de amenazas cibernéticas existente, las políticas y procedimientos de seguridad de la información de la institución y las responsabilidades de seguridad cibernética del individuo. Algunos reguladores, como la Autoridad Monetaria de Arabia Saudita (SAMA), exigen que las instituciones midan la eficacia de sus programas de sensibilización y fomenten la sensibilización de sus clientes como parte de esos programas. Otros reguladores, como el Banco de Israel, requieren que las instituciones también fomenten la conciencia de sus proveedores de servicios y que revisen sus programas periódicamente de acuerdo con el panorama de amenazas cibernéticas y la evaluación de riesgos correspondiente.

Fuerza laboral de seguridad cibernética

50. Los reguladores esperan que los bancos asignen recursos adecuados para implementar su marco de seguridad cibernética. Aunque elaborar expectativas con respecto a la experiencia en seguridad cibernética es bastante desafiante, dado que es probable que diferentes bancos tengan diferentes necesidades relacionadas con el personal de seguridad cibernética, muchos reguladores afirman que la implementación de un marco sólido de seguridad cibernética depende de la asignación de recursos adecuados, incluidos los recursos humanos con las habilidades necesarias para implementar la estrategia de seguridad cibernética. Hong Kong es único en el sentido de que ha establecido el Marco de competencias mejorado en ciberseguridad (ECF-C), que establece las competencias básicas comunes requeridas de los profesionales de seguridad cibernética en la industria bancaria de Hong Kong. Si bien el ECF-C no es obligatorio, se alienta a los bancos a adoptarlo para que la industria bancaria; i) desarrollar una reserva de talentos sostenible de profesionales de la ciberseguridad; y (ii) elevar y mantener la competencia profesional de los profesionales de la seguridad cibernética. También vale la pena señalar los esfuerzos de Carnegie para desarrollar capacidades con el lanzamiento en 2019 de una "Caja de herramientas de creación de capacidad de resiliencia cibernética para organizaciones financieras" junto con varias organizaciones asociadas.

51. Desde el punto de vista reglamentario y de supervisión, también es necesario garantizar que dispongan de los recursos necesarios para aplicar las normas de ciberseguridad. Idear regulaciones cibernéticas es la parte fácil porque se basan principalmente en estándares internacionales, pero hacer cumplir estas regulaciones es el verdadero desafío. El personal de supervisión debe ser capaz de evaluar adecuadamente si los bancos están siguiendo el espíritu de las regulaciones y no simplemente haciendo un ejercicio de marcar casillas. Esto implica atraer y retener personal con experiencia cibernética relevante, que es otro desafío para la comunidad reguladora. Para mitigar estos desafíos, los reguladores están utilizando diversos enfoques, como el desarrollo del talento interno a través de requisitos de desarrollo profesional (por ejemplo, MAS y Banco de Italia) y la centralización de sus especialistas en riesgos, incluidos los expertos en riesgos cibernéticos, en unidades individuales (por ejemplo, el Banco de Inglaterra). Sin embargo, según una encuesta del FMI, el 68% de las autoridades de 51 EMED carecen de una unidad de riesgo especializada en su departamento de supervisión.

Métricas de resiliencia cibernética

52. Los reguladores no suelen exigir a los bancos que presenten o supervisen métricas específicas de ciberresiliencia. Los pocos reguladores que lo hacen tienen requisitos de muy alto nivel. Por lo general, estos requisitos piden a los bancos que definan métricas que indiquen la efectividad de sus prácticas de seguridad cibernética o que destaquen los activos de información que tienen la mayor exposición al riesgo.

53. Cuando existe, el requisito de definir métricas e indicadores forma parte de las actividades de notificación, seguimiento, control y gestión de incidentes. APRA, por ejemplo, proporciona orientación práctica a sus bancos sobre qué tipos de información cuantitativa y cualitativa darían a las juntas y a la alta gerencia una imagen más clara de su seguridad cibernética. Por ejemplo, la guía establece que los resultados de las actividades de prueba de control y los eventos de seguridad detectados podrían ser parte de la información que podría proporcionarse a la junta y a la alta gerencia. El BSP, por otro lado, requiere que los bancos definan métricas o indicadores de posible compromiso para mejorar las capacidades de detección y monitoreo de fraude y facilitar la notificación de incidentes cibernéticos regulatorios. Esto podría incluir el acceso a un sistema altamente confidencial más allá del horario de oficina y los intentos fallidos de inicio de sesión de privilegiar las cuentas de usuario.

54. Los ejemplos de métricas mencionados en los reglamentos vigentes solo proporcionan información amplia sobre los enfoques de los bancos para crear y garantizar la ciberseguridad y la resiliencia. Esto demuestra que el desarrollo de métricas de resiliencia cibernética con fines de supervisión aún se encuentra en una etapa temprana. Sin embargo, la naturaleza del riesgo cibernético hace que un enfoque retrospectivo de las métricas de resiliencia cibernética sea ineficaz. Los jugadores de amenazas cibernéticas son dinámicos y se adaptan continuamente a las respuestas y medidas de protección. Por lo tanto, existe un creciente reconocimiento de la necesidad de indicadores prospectivos como métricas directas e indirectas de ciberseguridad y resiliencia.

Sección 5 – Conclusión

55. Las reglamentaciones bancarias relativas a la ciberseguridad y la ciberresiliencia han madurado y ya están bien establecidas en varias jurisdicciones. Las regulaciones relacionadas con la seguridad cibernética y la resiliencia cibernética cubiertas en Crisanto y Prenio (2017) eran bastante nuevas. Estas regulaciones existían solo en unas pocas jurisdicciones, principalmente en AES, y se centraban en establecer un enfoque y controles de gestión de riesgos cibernéticos. Seis años después, muchas jurisdicciones, incluidas las EMED, ya cuentan con regulaciones relacionadas con el ciberespacio. Muchas de estas regulaciones más recientes (o regulaciones cibernéticas de segunda generación) se centran en mejorar las capacidades de resiliencia cibernética y proporcionar a las instituciones y autoridades financieras herramientas para gestionar adecuadamente los riesgos cibernéticos. No obstante, un número importante de EMED todavía no tienen regulaciones relevantes.

56. Los reguladores están agregando requisitos o expectativas específicas en algunas áreas o agregando nuevos elementos en sus regulaciones cibernéticas. Ahora existen requisitos regulatorios más específicos sobre respuesta y recuperación de incidentes cibernéticos, así como sobre gestión y supervisión de terceros, informes de incidentes y marcos de prueba. Algunas jurisdicciones también han introducido requisitos o expectativas para la fuerza laboral de seguridad cibernética y las métricas de resiliencia cibernética. Sin embargo, la estrategia de seguridad cibernética, los informes de incidentes cibernéticos, el intercambio de inteligencia de amenazas, las dependencias de terceros y las pruebas de resiliencia cibernética siguen siendo el enfoque principal de estas regulaciones.

57. Las regulaciones cibernéticas en las EMED tienden a ser más prescriptivas. Este es especialmente el caso cuando se trata de la estrategia de seguridad cibernética, los acuerdos de gobernanza, incluidos los roles y responsabilidades, y la naturaleza y frecuencia de las pruebas de resiliencia cibernética. Los reguladores bancarios en las EMED tal vez vean la necesidad de fortalecer la cultura de resiliencia cibernética en todo el sector financiero y/o de ser más claros y específicos en sus expectativas dadas las limitaciones de recursos y el suministro limitado de habilidades y experiencia en sus jurisdicciones. De esta manera, los consejos de administración, la alta dirección y el personal de los bancos tienen una orientación concreta a seguir para mejorar la seguridad cibernética de sus instituciones.

58. Es necesario protegerse contra un enfoque basado en el cumplimiento para abordar la ciberseguridad. Demasiada prescriptividad puede resultar en un enfoque de casilla de verificación para la seguridad cibernética. La implementación de regulaciones cibernéticas tampoco debe verse como un ejercicio de casilla de verificación. Debe complementarse con recursos de supervisión adecuados para garantizar una aplicación y un cumplimiento efectivos. Por lo tanto, hay margen para que las organizaciones internacionales y las autoridades financieras en Aes apoyen los esfuerzos de desarrollo de capacidades de supervisión en las EMED, en particular en el ámbito de la ciberseguridad. Después de todo, las amenazas cibernéticas no conocen fronteras.

59. El trabajo internacional (por ejemplo, de los organismos de seguridad y del G7) ha facilitado un nivel útil de convergencia de la ciber resiliencia en el sector financiero, pero es necesario seguir trabajando. Ninguna empresa o regulador puede abordar con éxito el riesgo cibernético por sí solo. Además, la naturaleza transfronteriza del riesgo cibernético requiere un grado razonable de alineación en las expectativas regulatorias nacionales. El trabajo del G7 CEG y los SSB sobre ciberresiliencia ha hecho que las expectativas de regulación y supervisión financiera sean más consistentes en diferentes jurisdicciones y, por lo tanto, es un paso en la dirección correcta. En particular, la propuesta del FSB para una mayor convergencia en la notificación de incidentes cibernéticos es un desarrollo importante, ya que trata de conciliar los diferentes requisitos jurisdiccionales que solo cargan a las instituciones supervisadas en lugar de ayudar a abordar estos incidentes. En el futuro, podría haber margen para alinear las formas en que las autoridades evalúan la resiliencia cibernética de las instituciones supervisadas. Esto podría, por ejemplo, incluir alinear la evaluación de la adecuación de la gobernanza de seguridad cibernética, la fuerza laboral y las métricas de resiliencia cibernética de una empresa. Además, dadas las posibles implicaciones transfronterizas para el sistema financiero de un incidente cibernético en un proveedor externo crítico, particularmente un proveedor de nube, podría haber margen para considerar un marco de supervisión internacional para dichos proveedores.