Recuadro 4: Altos niveles de ciberresiliencia como factor clave para la estabilidad de las infraestructuras financieras

1. Introducción

Ante la creciente dependencia de las tecnologías de la información y las comunicaciones (TIC), la ciberseguridad y la ciberresiliencia se han convertido en prioridades para todos los sectores, y en particular para el financiero[1]. Las amenazas cibernéticas son cada día más frecuentes y sofisticadas[2], y afectan a diversos actores del sistema financiero, como por ejemplo las infraestructuras del mercado financiero (IMF), poniendo en riesgo su estabilidad e integridad, y por su potencial impacto sobre la estabilidad financiera se constituyen en una preocupación importante para las autoridades económicas (Doerr *et al*. 2022).

Teniendo en cuenta que la función que realizan las IMF es fundamental para la estabilidad financiera, al facilitar la liquidación y compensación de obligaciones en los mercados financieros, mantener su funcionamiento normal y seguro es una prioridad para las autoridades económicas. Para garantizar su operación continua y estable, las IMF deben mitigar su exposición a los riesgos que enfrentan, entre estos el cibernético, y por ende fortalecer su resiliencia.

Este recuadro presenta un marco conceptual sobre el análisis de riesgo cibernético con un especial énfasis en las IMF. Describe las preocupaciones y posibles acciones de las autoridades financieras por fortalecer la ciberresiliencia para la estabilidad de las IMF y, en general, del sector financiero. Para tal fin el recuadro se compone de cinco secciones adicionales a esta introducción. La segunda trata sobre los estándares internacionales establecidos para la gestión del riesgo y la resiliencia cibernética en las IMF. Las principales modalidades de ciberataques que enfrentan las instituciones financieras, y en particular las IMF, se describen en la tercera sección. La cuarta expone los factores a través de los cuales el ciberriesgo tiene el potencial para impactar la estabilidad financiera. Una compilación de las acciones emprendidas en el mundo y en Colombia, tanto por las autoridades financieras, como por el sector privado y los organismos multilaterales, se presentan en la quinta sección. En la sexta se presentan las conclusiones y recomendaciones.

2. Estándares internacionales para la gestión del riesgo y resiliencia cibernética en las IMF

La operación segura y eficiente de las IMF es esencial para mantener y promover la estabilidad financiera y el crecimiento económico. Si las IMF no gestionan adecuadamente sus riesgos, entre estos el cibernético, pueden convertirse en fuentes de choques financieros, como desajustes de liquidez y pérdidas crediticias, o en un canal a través del cual estos choques se transmiten en los mercados financieros nacionales e internacionales. En este contexto,

---

1 Aunque los términos de “ciberseguridad” y “ciberresiliencia” pueden parecer sinónimos, ya que ambos están relacionados con la protección contra ataques cibernéticos, sus acciones, herramientas y objetivos particulares difieren. De forma sencilla, mientras que la "ciberseguridad” hace referencia a la colección de tecnologías y acciones emprendidas con el objetivo de mitigar los riesgos de seguridad; el concepto de “ciberresiliencia” corresponde a la capacidad de la organización para recuperar datos, evitar la interrupción del servicio, mitigar los daños generales y al mismo tiempo garantizar la exitosa recuperación frente a eventos cibernéticos adversos.

2 En los reportes de riesgos futuros publicados por AXA de los últimos cinco años (2018-2022), el de ciberseguridad se ha posicionado entre los tres principales riesgos, según los resultados de la encuesta realizada a expertos y al público en general. La alta dependencia de la tecnología en nuestras vidas hace que los riesgos de seguridad cibernética, como la salud, sean una inquietud duradera. Asimismo, las tensiones geopolíticas actuales alimentan directamente la preocupación por los riesgos cibernéticos. En su reporte de 2022, las principales preocupaciones de los expertos por este riesgo fueron: las del cierre de servicios esenciales e infraestructura crítica, el robo de identidad (personal y corporativa) y la extorsión cibernética y el *ransomware* (secuestro de datos). Por su parte, el público encuestado comparte las dos primeras preocupaciones de los expertos e incluyen a la violación de la privacidad como adicional; véase: https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/15c65a87-4d11-49a4-b88e-be5953965b37_axa_futurerisksreport_2022_va.pdf

el nivel de ciberresiliencia de las IMF contribuye a la continuidad en la prestación de sus servicios, y puede ser un factor decisivo en la resiliencia general del sistema financiero y la economía en general.

Los Principios para las Infraestructuras del Mercado Financiero (PIMF), publicados en abril de 2012 por el Comité de Sistemas de Pago y Liquidación (CPMI) y el Comité Técnico de la Organización Internacional de Comisiones de Valores (Iosco) (CPMI-Iosco 2012), definieron como principal objetivo de política pública "mejorar la seguridad y la eficiencia en los acuerdos de pago, compensación, liquidación y registro y, en términos más generales, limitar el riesgo sistémico y fomentar la transparencia y la estabilidad financiera". Respecto al riesgo cibernético, los PIMF reconocieron que este hace parte de los riesgos operativos y establecieron que una IMF debe contar con disposiciones y objetivos de gobernanza para gestionar estos riesgos dentro de un marco integral de gestión de riesgos.

En junio de 2016 el CPMI-Iosco publicó la "Guidance on Cyber Resilience for Financial Market Infrastructures" (en adelante: la guía), en la cual atiende de manera particular al riesgo cibernético, y formula orientaciones a las IMF para mejorar su ciberresiliencia con el objetivo de limitar los riesgos crecientes que las amenazas cibernéticas representan para la estabilidad financiera. La ciberresiliencia se define allí como: "la capacidad de una IMF para anticipar, soportar, contener y recuperarse rápidamente de un ciberataque".

Específicamente, la guía CPMI-Iosco (2016) ofrece una orientación complementaria a los PIMF, pero no pretende imponer a las IMF estándares adicionales a los establecidos en los PIMF, sino que proporciona detalles adicionales relacionados con medidas que las IMF deben realizar para mejorar sus capacidades de ciberresiliencia. Principalmente, las orientaciones complementarias se dan a los PIMF en el contexto de la gobernanza (principio 2), el marco para la gestión integral de riesgos (principio 3), la finalización de liquidaciones (principio 8), el riesgo operacional (principio 17) y los vínculos de las IMF (principio 20)[3].

Al respecto, la guía define[4] al riesgo cibernético como: "la combinación de la probabilidad de que ocurra un evento dentro del ámbito de los activos de información, los recursos informáticos y de comunicación de una organización y las consecuencias de ese evento para una organización", e identifica características únicas de este riesgo, como son: 1) la naturaleza persistente de una campaña realizada por un atacante motivado (ataque malicioso); 2) la existencia de una amplia gama de puntos de entrada a través de los cuales una IMF podría verse comprometida (participantes de una IMF, las IMF vinculadas, los proveedores de servicios, los vendedores y los productos de los vendedores, empleados descuidados y/o deshonestos); 3) ciertos ataques cibernéticos pueden hacer que algunos arreglos de gestión de riesgos y continuidad comercial sean ineficaces (sistemas automatizados y los arreglos de replicación de datos contaminados), y 4) los ataques cibernéticos pueden ser sigilosos y propagarse rápidamente dentro de una red de sistemas (explotar vulnerabilidades desco-

3 Principio 2. Gobierno corporativo: una IMF deberá contar con mecanismos de gobierno corporativo que sean claros y transparentes, que promuevan la seguridad y eficiencia de la IMF y respalden la estabilidad del sistema financiero en general, otras consideraciones de interés público relevantes y los objetivos de las partes interesadas relevantes.

Principio 3. Marco para la gestión integral de riesgos: una IMF deberá contar con un sólido marco de gestión de riesgos para gestionar integralmente los riesgos legales, crediticios, de liquidez, operativos y de otro tipo.

Principio 8. Finalidad de la liquidación: una IMF deberá proporcionar una liquidación definitiva clara y segura, como mínimo al final de la fecha de valor. Cuando sea necesario o preferible, una IMF deberá proporcionar la liquidación final intradía o en tiempo real.

Principio 17. Riesgo operativo: una IMF deberá identificar las posibles fuentes de riesgo operativo, tanto internas como externas, y mitigar su impacto mediante el uso de sistemas, políticas, procedimientos y controles apropiados. Los sistemas deben diseñarse para garantizar un alto grado de seguridad y confiabilidad operativa y deben tener una capacidad escalable adecuada. La gestión de la continuidad del negocio deberá tener como objetivo la recuperación oportuna de las operaciones y el cumplimiento de las obligaciones de la IMF, incluso en el caso de una interrupción importante o a gran escala.

Principio 20. Vínculos de las IMF: una IMF que establezca un vínculo con una o más IMF deberá identificar, controlar y gestionar los riesgos relacionados con los vínculos.

4 Una definición alternativa es la del *Cyber Lexicon* del Consejo de Estabilidad Financiera (FSB por su sigla en inglés), en la que el riesgo cibernético se refiere a "la combinación de la probabilidad de que ocurran incidentes cibernéticos y su impacto", y donde un "ciberincidente" corresponde a "cualquier ocurrencia observable en un sistema de información [...] que: (i) pone en peligro la seguridad cibernética de un sistema de información o la información que el sistema procesa, almacena o transmite; o (ii) viole las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable, ya sea como resultado de una actividad maliciosa o no".

nocidas y enlaces débiles en sistemas y protocolos para causar interrupciones y/o infiltrarse en la red interna de una IMF).

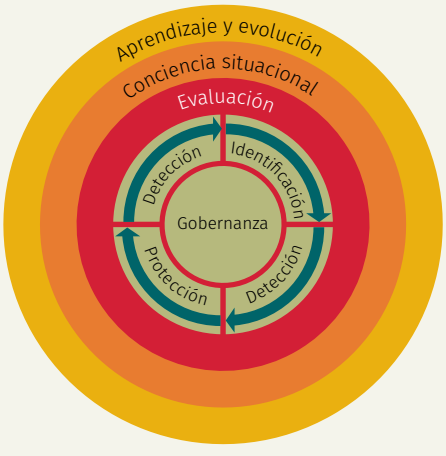
La guía recomienda a las IMF implementar un marco de ciberresiliencia que se acople a la naturaleza dinámica de los riesgos cibernéticos y promueva una cultura de conciencia de riesgo cibernético. Las IMF deben implementar la guía mediante un enfoque basado en el riesgo y desarrollar planes concretos para mejorar sus capacidades, incluido el cumplimiento del objetivo de tiempo de recuperación de dos horas.

La comprensión de las vulnerabilidades de la estabilidad financiera que se derivan de incidentes cibernéticos es fundamental, como lo postula Brando et al. (2022), ya que mientras que el capital y la liquidez pueden ser suficientes para atender eventos de pérdidas financieras, ante un incidente cibernético resultan insuficientes para acelerar el proceso de recuperación de sistemas o datos.

Las ramificaciones sistémicas ante la materialización del riesgo cibernético pueden superar a las del riesgo operativo, pues como lo reconoce Brando et al. (2022), reacciones como las ventas forzadas, el congelamiento de la liquidez, los posibles problemas de solvencia y la recuperación del flujo normal de los pagos pueden evolucionar de manera diferente después de un choque cibernético. Un incidente cibernético en una institución financiera puede comprometer sus datos y su capacidad para atender a los acreedores y ocasionar que sus clientes corran a otras instituciones por temor a la falta de acceso a las cuentas.

Por su parte la guía de CPMI-Iosco (2016) formula orientaciones a las IMF (Diagrama R4.1) sobre resiliencia cibernética, y les recomienda incluir como categorías dentro de su gestión de riesgos: gobernanza sólida, identificación de funciones críticas y activos a proteger, protección de confidencialidad, integridad, y disponibilidad de activos y servicios de un IMF, detección de incidentes cibernéticos y la reanudación segura de operaciones críticas en dos horas.

Diagrama R4.1
Componente de la guía de ciber resiliencia



Fuente: CPMI-Iosco (2016).

Adicionalmente, la guía CPMI-Iosco (2016) aconseja a las IMF incluir en la definición del marco de ciberresiliencia componentes generales como:

a. Pruebas: los elementos del marco de ciberresiliencia de una IMF deben ser rigurosamente probados para determinar su eficacia general.

b. Conciencia situacional: las IMF deben monitorear proactivamente el panorama de amenazas cibernéticas y utilizar información sobre amenazas para validar sus evaluaciones de riesgo y estrategias de mitigación.

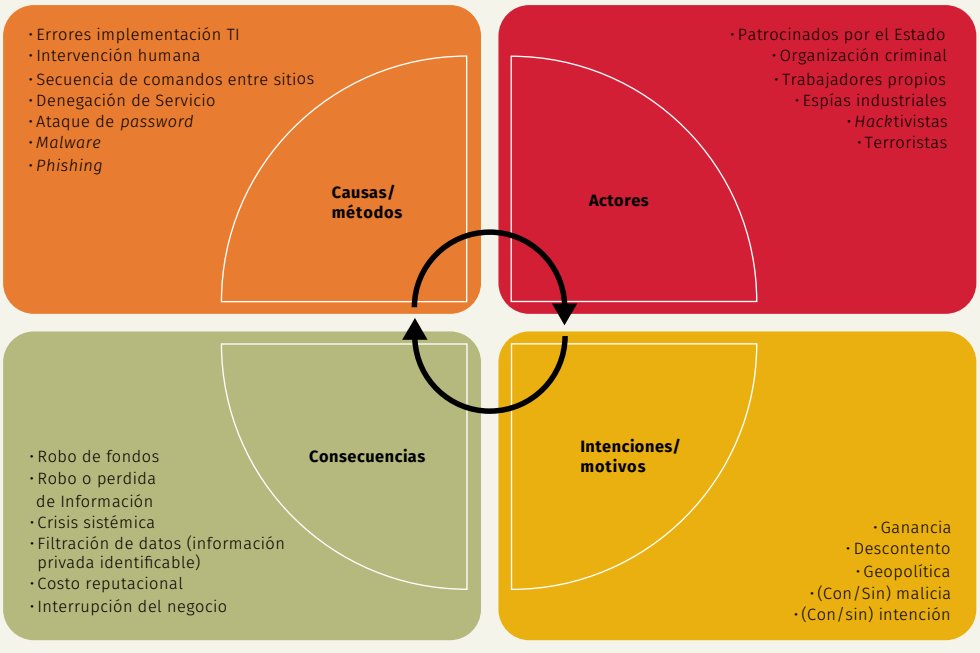
c. Aprendizaje y evolución: las IMF deben implementar un marco de ciberresiliencia adaptable que evolucione con la naturaleza dinámica de los riesgos cibernéticos.

3. Taxonomía del ciberriesgo en el sistema financiero

El riesgo cibernético al que se enfrentan las instituciones financieras y las IMF puede ser clasificado bajo la taxonomía simple propuesta por Aldasoro *et al.* (2022), el cual tiene en cuenta cuatro categorías: causas/métodos, actores, motivos/intenciones y consecuencias (Diagrama R4.2).

Dentro de las causas se incluyen tanto incidentes no intencionados como ataques intencionados. A manera de ejemplo, en el sector financiero se incluye la divulgación accidental de datos, así como errores en la implementación, configuración y procesamiento de las

Diagrama R4.2
Taxonomía simple del riesgo cibernético



Fuente: Aldasoro et al. (2022).

TIC. En cuanto a los métodos con que se realizan ciberataques al sistema financiero, los más comunes son el *ransomware*, el robo de datos, *malware*, las secuencias de comandos entre sitios, la suplantación de identidad (*phishing*), el descifrado de contraseñas y los ataques de denegación de servicio.

Entre los actores están los patrocinados por el Estado[5], las organizaciones criminales y terroristas, los espías industriales y grupos de *hacktivistas* (como Anonymous). En cuanto a la intencionalidad, según Aldasoro *et al*. (2020), cerca del 40% de los incidentes cibernéticos son intencionados y maliciosos, más que accidentales, y persiguen fines lucrativos (por ejemplo, *ransomware*, espionaje industrial), geopolítico (ataques patrocinados por el Estado a infraestructuras críticas) o expresan discordia general.

Los bancos centrales, según Doerr *et al*. (2022), con base en una encuesta realizada en 2021 entre los miembros del Global Cyber Resilience Group (GCRG)[6], consideran que el *phishing* y la ingeniería social son los métodos de ataque más comunes, y que las pérdidas potenciales

5 Un ataque cibernético patrocinado por un Estado es una forma de estrategia de defensa adoptada por las naciones para atacar a los gobiernos, la infraestructura crítica y la sociedad civil de Estados hostiles. En este tipo de ataques son famosos los realizados por los gobiernos de Corea del Norte, Rusia y Ucrania.

El Departamento del Tesoro de Estados Unidos reconoce que en el caso de Corea del Norte operan como agencias controladas por el gobierno los grupos Lazarus, Bluenoroff y Andariel. El grupo Lazarus se especializa en ataques a instituciones gubernamentales, militares, financieras, manufactureras, editoriales, de medios de comunicación, de entretenimiento y compañías navieras internacionales, así como en infraestructura crítica, utilizando tácticas como ciberespionaje, robo de datos, atracos monetarios y operaciones destructivas de *malware*. Este grupo estuvo involucrado en el *ransomware* conocido como Wannacry 2.0 en 2017, el cual afectó a 150 países y apagó aproximadamente trescientos mil computadoras. El grupo Bluenoroff fue formado por el gobierno de Corea del Norte para obtener ingresos de forma ilícita como respuesta al aumento de las sanciones globales. Junto con Lazarus, este grupo realizó el robo de USD 80 millones al Banco de Bangladesh utilizando credenciales robadas del sistema Swift. Por su parte Andariel se enfoca en operaciones cibernéticas maliciosas contra empresas extranjeras, agencias gubernamentales, infraestructura de servicios financieros, corporaciones y negocios privados, así como en la industria de defensa. Este grupo fue identificado en el intento de robo de información de tarjetas bancarias, al piratear cajeros automáticos para retirar efectivo o robar información de clientes para luego venderla en el mercado negro, y también ha sido responsable de desarrollar y crear *malware* único para piratear sitios de apuestas y póquer en línea para robar dinero en efectivo. Tomado de https://home.treasury.gov/news/press-releases/sm774

Este tipo de ataques patrocinados por el Estado se han incrementado no solo durante la guerra Rusia-Ucrania, sino que cobraron relevancia desde la pandemia por covid19. Los ciberataques rusos dirigidos a los países de la OTAN y a Ucrania en 2022 fueron cuatro y tres veces, respectivamente, los registrados en 2020.

6 Conformada por bancos centrales de nueve economías avanzadas y doce de economías emergentes.

de un ataque cibernético adquieren una dimensión sistémica importante cuando se dirigen a empresas tecnológicas que proveen, más que servicios financieros, servicios digitales a infraestructuras críticas en la nube.

En la misma encuesta, Doerr *et al*. (2022) encuentran que los bancos centrales de economías avanzadas están más preocupados por los ataques a la cadena de suministro[7] que sus homólogos de economías emergentes, y que cuando se trata de los costos resultantes de un ataque, los bancos centrales coinciden en que los ataques avanzados de *malware* y *ransomware* persistentes ocupan los primeros lugares. Respecto a la autoría de los ataques, los bancos centrales de economías avanzadas consideran al crimen organizado y a grupos maliciosos patrocinados por el Estado como los principales perpetradores, mientras que para los de economías emergentes lo son el crimen organizado y *hacktivistas* individuales.

Los incidentes cibernéticos pueden tener consecuencias monetarias o reputacionales sobre las IMF, las cuales se traducen en la pérdida de fondos, de confidencialidad y de disponibilidad de servicios. Ataques maliciosos concebidos como fraude y robo incluyen la pérdida de fondos o de información. Ataques cibernéticos a las IMF pueden, por su papel fundamental en el sistema financiero y en la economía en general, desencadenar impactos sistémicos y causar graves consecuencias económicas que terminan afectado la estabilidad financiera.

4. Ciberriesgo como fuente de vulnerabilidad financiera

El riesgo cibernético plantea una preocupación cada vez mayor en relación con las IMF y su impacto en la estabilidad financiera. El papel central que desempeñan las IMF en el sistema financiero las convierte en un componente central y altamente interconectado. Su alta dependencia de tecnologías de información y de comunicaciones las expone a riesgos cibernéticos significativos que pueden desencadenar efectos sistémicos sobre participantes, otras IMF y mercados financieros. El riesgo cibernético en IMF e instituciones financieras tiene el potencial de impactar significativamente la estabilidad financiera debido a factores tales como:

1. Propagación a través del sistema financiero: los ciberataques pueden propagarse a través de conexiones complejas y no reconocidas entre empresas. Dichas conexiones resultan de la utilización de tecnologías compartidas y de proveedores de servicios de terceros, así como de las redes que se forman entre entidades financieras por los pagos realizados y por las exposiciones por riesgo de contraparte (Brando *et al*. 2022). Para Adelmann *et al*. (2020) el mecanismo de propagación de ciberataques exitosos sobre IMF en el sistema financiero es debido a que estas, al facilitar las labores de compensación y liquidación, establecen conexiones con participantes responsables de un gran volumen de transacciones diarias en diferentes mercados y altamente dependientes de la tecnología, a través de las cuales pueden impactar a otros participantes directos, otras IMF y sus clientes, así como a mercados.

2. Concentración del mercado: el aumento de la concentración del mercado, impulsado por economías de escala digitales u otras fuerzas del mercado, puede generar puntos críticos de falla y una mayor vulnerabilidad del sistema financiero ante las crisis cibernéticas. Esto se evidencia en servicios clave como la compensación y liquidación, así como en la prestación de servicios en la nube. Además, el incremento de las transacciones compensadas a través de entidades de contrapartida central (ECC) representa un mayor riesgo de vulnerabilidad cibernética debido a la concentración de la actividad en una sola entidad y su dependencia de la inversión en resiliencia cibernética.

3. Naturaleza de la intención de los ciberataques: los ciberataques pueden tener diferentes intenciones, algunos persiguen fines lucrativos, mientras que otros, respaldados por Estados-nación con capacidades de ciberataque, buscan causar el mayor daño posible. En el caso de ataques respaldados por Estados-nación, su objetivo puede ser destruir o

7 Cuando el ataque cibernético se dirige a la cadena de suministro, el actor de la amenaza se infiltra en la red de un proveedor de *software* legítimo y mediante un código malicioso compromete el *software* antes de que el proveedor lo distribuya a sus clientes. Estos ataques aprovechan la confianza depositada y las comunicaciones máquina a máquina que se dan en las actualizaciones esenciales de *software*. Por su dificultad de mitigar, se dirigen tanto a proveedores de servicios (por ejemplo, el ataque a la compañía de *software* e infraestructura de redes SolarWinds de 2020) como a tecnologías clave (por ejemplo, los servidores de Microsoft Exchange en 2021). Los ataques a la cadena de suministro son menos frecuentes, pero pueden tener consecuencias graves y potencialmente sistémicas (Doerr *et al*. 2022)

suspender por periodos prolongados las operaciones del sistema objetivo. Esta situación puede hacer que, incluso con inversiones considerables en resiliencia, el sistema financiero sea más vulnerable si hay menos redundancias o si faltan sustitutos adecuados para IMF o instituciones financieras, lo que puede generar un mayor contagio.

4. Exposiciones de riesgo correlacionadas: las exposiciones de riesgo correlacionadas pueden impactar la estabilidad financiera. Por ejemplo, si varias empresas utilizan la misma actualización de *software* de terceros infectada con *malware*, pueden generar simultáneamente pérdidas en múltiples empresas. Debido a las interconexiones en el sistema financiero, esto puede tener un efecto dominó y afectar de manera sistémica a otras entidades.

5. Efectos en cascada: similar a los problemas operativos o de liquidez, un evento cibernético en un banco puede interrumpir su capacidad para enviar pagos, lo que puede tener efectos en cascada en la liquidez y las operaciones de otras entidades financieras. Además, las empresas individuales que en la cadena de suministros proveen servicios (energía, telecomunicaciones, *hardware* y *software*) al sistema financiero, al no invertir adecuadamente en ciberresiliencia y al no internalizar el impacto de sus acciones sobre la estabilidad del sistema, exponen al sistema financiero a un riesgo superior al óptimo.

En conclusión, el riesgo cibernético representa una amenaza significativa para la estabilidad financiera debido a su propagación a través del sistema financiero, la concentración del mercado, la intención de los ciberataques, las exposiciones de riesgo correlacionadas y los efectos en cascada.

5. Acciones emprendidas para la mitigación del riesgo cibernético y el fortalecimiento de la ciberresiliencia

La mitigación del riesgo cibernético y sus vulnerabilidades sistémicas requiere de un enfoque integral que involucre los reguladores, supervisores y el sector privado (instituciones financieras e IMF), en pro de mejorar la resiliencia operativa, la promoción de la resiliencia cibernética mediante la supervisión financiera, la colaboración en iniciativas lideradas por el sector privado y el desarrollo de mercados de seguros cibernéticos.

Aldasoro *et al*. (2022) agrupa en cuatro áreas principales las acciones emprendidas por diversos tipos de organizaciones para mitigar el riesgo de ciberataques y fortalecer la ciberresiliencia:

1. Fortalecimiento de la resiliencia operativa: tanto las organizaciones del sector público como del privado están trabajando para mejorar su capacidad de resistir y recuperarse de incidentes cibernéticos. Esto implica alinear las actividades de seguridad con los objetivos empresariales y priorizar las inversiones en ciberseguridad. Además, como mecanismo para reforzar la resiliencia, se fomenta la mentalidad de asumir una desconfianza continua en los niveles operativos y de gobernanza. Las organizaciones también pueden aprender unas de otras compartiendo conocimientos. En esta línea de acción está el Centro de Coordinación de Resiliencia Cibernética que el BIS conformó con el objetivo de fomentar el intercambio de información y la colaboración entre los bancos centrales.

2. Promoción de la resiliencia cibernética mediante la supervisión financiera: los supervisores y reguladores financieros utilizan estándares y guías nacionales o internacionales para fomentar la resiliencia cibernética en las instituciones financieras. Muchas autoridades utilizan herramientas regulatorias y supervisoras existentes para establecer expectativas en la gestión, evaluación y respuesta a riesgos cibernéticos. Algunos incluso participan en pruebas o simulaciones de incidentes cibernéticos reales en cooperación con el sector financiero.

3. Iniciativas lideradas por el sector privado: el sector privado adelanta varias iniciativas para apoyar la cooperación y coordinación en la prevención, respuesta y recuperación de incidentes cibernéticos, así como en el intercambio de información. Para ayudar a mitigar los riesgos cibernéticos que se generan de la dependencia en la prestación de servicios en nube por parte de terceros, las instituciones financieras están colaborando en marcos para la portabilidad de datos y la interoperabilidad entre proveedores de este tipo de servicios.

4. Desarrollo de mercados de seguros cibernéticos: este mercado está en crecimiento y podría ayudar a las empresas a cubrir pérdidas y fomentar mejoras en la resiliencia cibernética. Sin embargo, dicha cobertura puede ser insuficiente para evitar grandes riesgos extremos, e incluso podría contribuir a la propagación de pérdidas a partir de impactos sistémicos.

El Comité de Supervisión Bancaria de Basilea y el BIS (BCBS-BIS, 2018) ante un entorno de creciente dependencia de las TIC y la externalización de servicios a terceros, evaluaron las prácticas de ciberresiliencia en bancos, reguladores y supervisores en diferentes jurisdicciones. El objetivo del informe fue identificar, describir y comparar las prácticas de ciberresiliencia en diferentes jurisdicciones, utilizando información de encuestas realizadas por la Junta de Estabilidad Financiera (FSB) y la experiencia directa de los miembros del Grupo de Trabajo de Resiliencia Operacional (ORG) (Cuadro R4.1).

Con base en los resultados del informe se diseñaron iniciativas internacionales para aumentar la ciberresiliencia, como los Elementos Fundamentales de Ciberseguridad del G7 (Group of Seven, 2016) y la orientación de CPMI-Iosco para IMF. Para la Unión Europea, el Plan de Acción Fintech de la Comisión Europea (European Systemic Risk Board, 2020) exhortó a las autoridades supervisoras europeas a considerar la emisión de directrices para lograr la convergencia en el riesgo de las TIC.

En este contexto, el Comité de Supervisión Bancaria de Basilea (BCBS) reconoció los méritos de abordar la resiliencia operativa más allá del ámbito de la gestión del riesgo operativo y los requisitos mínimos de capital, y estableció el Grupo de Trabajo de Resiliencia Operacional (ORG, por su sigla en inglés) con la intención de contribuir a, entre otras cosas, el esfuerzo internacional relacionado con el riesgo cibernético en estrecha coordinación con los demás organismos internacionales involucrados. Por tal razón, el BCBS solicitó que el ORG proporcione una primera evaluación de las prácticas de resiliencia cibernética observadas en las autoridades y de las instituciones financieras reguladas, incluidas las IMF.

En Colombia la ciberseguridad y la ciberresiliencia son temas de gran importancia debido al crecimiento del sector financiero y al aumento de la digitalización de los servicios financieros. El gobierno colombiano ha implementado estrategias y políticas nacionales para mejorar la ciberseguridad y la ciberresiliencia en el país, incluyendo la creación de la Estrategia Nacional de Ciberseguridad y Ciberdefensa en 2011 y la Comisión Intersectorial de Ciberseguridad en 2016.

Cuadro R4.1
Ciberresiliencia: rango de prácticas

1. Panorama general: la mayoría de los supervisores utilizan estándares nacionales o internacionales, como el marco NIST, la serie ISO 27000 y la guía CPMI-Iosco. Aunque hay convergencia en ciertas áreas, las especificaciones técnicas y prácticas varían entre jurisdicciones.	2. Estrategias: los reguladores no exigen una estrategia de ciberseguridad específica, pero esperan que las instituciones mantengan una capacidad adecuada como parte de sus estrategias globales.
3. Administración de ciberriesgo: a pesar de la madurez en la gestión de riesgos de TIC y operacionales, los bancos carecen de una estrategia de ciberseguridad que defina niveles claros de tolerancia y apetito al riesgo.	4. Gobernanza/organización: aunque se adoptan modelos, como el de las tres líneas de defensa (3LD), la ciberresiliencia no siempre se articula claramente en las diferentes áreas.
5. Fuerza laboral: la escasez de habilidades en ciberseguridad crea desafíos en la contratación de personal especializado.	6. Evaluación: las pruebas de protección y detección son prevalentes, pero las de respuesta y recuperación son menos comunes.
7. Capacidad de respuesta a incidentes: se espera que los bancos tengan planes de respuesta a incidentes, aunque no se requiere un marco de gestión de incidentes.	8. Métricas de ciberresiliencia: no existe un conjunto estándar de métricas para la ciberresiliencia, lo que dificulta la comunicación entre supervisores y bancos.
9. Intercambio información: la mayoría de los mecanismos de intercambio de información son entre bancos, y entre bancos y reguladores. Sin embargo, el contenido y uso de la información varía ampliamente entre jurisdicciones.	10. Riesgo de proveedores de servicios tercerizados: aunque hay marcos regulatorios comunes para la subcontratación, no hay un enfoque común para la gestión de riesgos de terceros más allá de los servicios externalizados.

Fuente: BCSB-BIS (2018); elaboración del Banco de la República.

La Superintendencia Financiera de Colombia (SFC) ha establecido normativas y directrices específicas para la ciberseguridad y la ciberresiliencia en el sector financiero. Estas regulaciones incluyen requisitos mínimos para la gestión del riesgo de ciberseguridad, como por ejemplo contar con políticas, procedimientos y recursos técnicos y humanos adecuados. La SFC sugiere el uso de estándares internacionales[8] para el desarrollo de sistemas de gestión de ciberseguridad.

En 2020 la SFC emitió la Resolución 0674, que establece un protocolo de crisis o contingencia para el mercado de valores y de divisas en el país, el cual fue un resultado del trabajo y acuerdos entre diferentes actores de la industria financiera. Este protocolo se enfoca en la gestión del riesgo operativo y tecnológico, incluyendo la ciberseguridad, la interrupción de operaciones y la recuperación de la información. Su objetivo es garantizar la continuidad de las operaciones en el mercado financiero a través de la identificación, prevención, monitoreo y gestión adecuada de los riesgos operativos y tecnológicos.

El Banco de la República (Banrep) también ha realizado una autoevaluación de sus capacidades de ciberseguridad basada en el Cyber Security Framework de NIST. El Banrep prioriza la integridad de los datos y se reserva el derecho de interrumpir la operación para investigar y garantizar la integridad y calidad de la información en sistemas y plataformas críticas. Además, está trabajando en un protocolo de gestión de desastres cibernéticos para sus servicios críticos.

Consciente del potencial impacto sistémico que sobre la estabilidad financiera puede ejercer la materialización del riesgo cibernético, el Banrep recientemente inició el monitoreo de las medidas que toman los establecimientos de crédito para protegerse frente a este tipo de riesgo. Para tal fin hace seguimiento a la calificación global del indicador de riesgo cibernético (IRC) que da el Security Scorecard, así como a los factores que lo componen[9].

Desde la iniciativa privada, Asobancaria, como gremio representativo del sector financiero colombiano, ha establecido un equipo sectorial de respuesta a incidentes, llamado CSIRT Financiero. Este equipo colaborativo fortalece la capacidad de anticipar, contener y mitigar los riesgos de ciberseguridad en entidades financieras y sistemas de pago.

En resumen, en Colombia se han implementado estrategias y regulaciones para mejorar la ciberseguridad y la ciberresiliencia en el sector financiero local. Tanto el Gobierno como las entidades reguladoras y el sector privado están trabajando en conjunto para combatir el cibercrimen y promover un ecosistema de colaboración en materia de ciberseguridad.

6. Conclusiones y recomendaciones

La ciberresiliencia es un aspecto crítico para garantizar la estabilidad y la integridad de las IMF en un mundo cada vez más interconectado y digitalizado. Los riesgos y amenazas cibernéticas evolucionan constantemente, lo que requiere una adaptación y mejora continuas de las estrategias de ciberseguridad y ciberresiliencia.

El riesgo cibernético se constituye en una amenaza significativa para la estabilidad financiera por diversas razones, como son: la compleja red de conexiones con la que se propaga a través del sistema financiero, la concentración del mercado, la intención de los ciberataques, las exposiciones de riesgo correlacionadas y los efectos en cascada.

El análisis de las amenazas cibernéticas y los enfoques para abordar los riesgos y desafíos asociados con la ciberseguridad en las IMF demuestra la necesidad de una aproximación holística y colaborativa en el manejo del tema. Las IMF e instituciones financieras, junto con las autoridades, supervisores y bancos centrales, deben trabajar coordinadamente para adoptar y mantener prácticas sólidas de ciberseguridad y ciberresiliencia como mecanismo que con-

8 Entre los que incluye la ISO 27032, NIST, ISF, CIS Critical Security Controls o Cobit 5 for Information Security.

9 Un mayor detalle de la metodología de cálculo del indicador de riesgo cibernético (IRC) y el análisis de resultados recientes para las entidades que componen el sistema financiero colombiano está disponible en el Recuadro 2: indicador de riesgo cibernético del Reporte de Estabilidad Financiera del I Semestre de 2023. https://repositorio.banrep.gov.co/bitstream/handle/20.500.12134/10638/reporte-estabilidad-financiera-primer-semestre-2023.pdf

tribuya a salvaguardar la estabilidad financiera. Esto incluye la adopción de marcos y estándares de ciberseguridad reconocidos, la promoción de la concientización y la formación en ciberseguridad, y el intercambio de información y colaboración con otros actores relevantes.

Los organismos multilaterales, como el BIS, el Banco Mundial y el FMI, también desempeñan un papel importante en la promoción de la ciberresiliencia en las IMF mediante el desarrollo de directrices y principios específicos, así como la provisión de asesoramiento y asistencia técnica en esta área.

Por consiguiente, es importante que las IMF y sus participantes a nivel local continúen trabajando y fortaleciendo acciones tales como: 1) mejorar la resiliencia cibernética, 2) fortalecer la colaboración e intercambio de información, 3) evaluar y gestionar los riesgos asociados con la provisión de servicios informáticos tercerizados, 4) fomentar la capacitación en seguridad cibernética, 5) fortalecer medidas de contingencia y planes de recuperación, y 6) realizar pruebas de contingencia y simulacros de ciberataques.

Entre esta línea de acciones, el Banrep adelanta una agenda de investigación dirigida a cuantificar el impacto sistémico que sobre el comportamiento en la liquidación y compensación tendría la materialización del riesgo cibernético en las IMF y/o en sus participantes y formular mecanismos y recomendaciones de política que permitan mitigarlo.

Al abordar estos desafíos y adoptar un enfoque proactivo hacia la gestión del riesgo cibernético, las IMF e instituciones financieras pueden reducir la probabilidad de un impacto significativo en la estabilidad financiera. La colaboración entre los sectores público y privado, así como una mayor conciencia y preparación, son fundamentales para proteger la infraestructura financiera de las amenazas cibernéticas en continua evolución.

Referencias

Adelmann, F.; Elliot, J.; Ergen, I.; Gaidosch, N.; Khiaonarong, T.; Morozova, A.; Schwarz, N.; Wilson, C. (2020). “Cyber Risk and Financial Stability: It’s a Small World after All”- December 2020. IMF Staff discussion note.

Aldasoro I., Gambacorta L., Giudici P. and Leach T. (2020). “The Drivers of Cyber Risk”, BIS Working Papers, 865, May.

Aldasoro I., Frost J., Gambacorta L., Leach T., and Whyte K. (2022) “Cyber Risk in the Financial Sector”- November 2020. SUERF Policy Note Issue No 206.

Brando D., Kotidis A., Kovner A., Lee M., and Schreft S. L. (2022). “Implications of Cyber Risk for Financial Stability,” FEDS Notes. Washington: Board of Governors of the Federal Reserve System, May 12, 2022. https://doi.org/10.17016/2380-7172.3077

BCBS-BIS (2018) “Cyber Resilience: Range of Practices” December. https://www.bis.org/bcbs/publ/d454.pdf

CPMI-Iosco (2012) “Principles for Financial Market Infrastructures” - April 2012, https://www.bis.org/cpmi/publ/d101a.pdf

CPMI-Iosco (2016) “Guidance on Cyber Resilience for Financial Market Infrastructures” - June 2016 https://www.bis.org/cpmi/publ/d146.pdf

Doerr, S., Gambacorta, L., Leach, T., Legros B., y Whyte D. (2022) “Cyber Risk in Central Banking” BIS Working Papers No 1039 September 2022 https://www.bis.org/publ/work1039.pdf

European Systemic Risk Board (ESRB) (2020). “Systemic Cyber Risk”, February 2020.

Group of Seven G7 (2016) “Fundamental Elements of Cybersecurity for the Financial Sector”, October 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/559186/G7_Fundamental_Elements_Oct_2016.pdf