Recuadro 3
DESARROLLOS RECIENTES REFERIDOS AL RIESGO DE CIBERSEGURIDAD

El *National Institute of Standards and Technology* (NIST) define al riesgo de ciberseguridad como "el riesgo de pérdida de confidencialidad, integridad o disponibilidad de datos o sistemas de información o control, y refleja los potenciales efectos adversos en las operaciones de las organizaciones (misión, funciones, imagen o reputación)"[7].

Riesgo de ciberseguridad y estabilidad financiera

En un artículo publicado en el portal del Fondo Monetario Internacional (FMI), Elliott y Jenkinson (2020)[8] explican que "con el aumento de la dependencia de servicios financieros digitales, el número de ciberataques se ha triplicado en la última década, y el sector de servicios financieros sigue siendo el blanco preferido. La ciberseguridad se ha convertido en una amenaza para la estabilidad financiera". Los mismos autores agregan que "dada la gran interconexión tecnológica y financiera, un ataque a una institución financiera importante, o a un sistema o servicio central muy utilizado, podría propagarse con rapidez por todo el sistema financiero, causando una perturbación generalizada y la pérdida de confianza. Las transacciones no se llevarían a cabo debido a que la liquidez estaría retenida, y los hogares y empresas podrían perder el acceso a los depósitos y los pagos. En casos extremos, los inversionistas y depositantes podrían exigir la retirada de sus fondos o tratar de cerrar sus cuentas u otros servicios y productos que suelen utilizar".

En el mismo sentido, Christine Lagarde (2018)[9] señala que "el riesgo cibernético se ha convertido en una amenaza importante para el sistema financiero". Un estudio basado en modelos realizado por el personal técnico del FMI estima que, en promedio, las pérdidas anuales de las instituciones financieras causadas por ataques cibernéticos podrían llegar a varios cientos de miles de millones de dólares, lo que representa un deterioro de las ganancias bancarias y una amenaza para la estabilidad financiera".

Como reflejo de ello, en diversas encuestas realizadas a gestores de riesgos y directivos del sector financiero, el riesgo de ciberseguridad es considerado uno de los más importantes, por encima de otros riesgos como el geopolítico o de cambios en la normativa[10].

Índices de ciberseguridad

El *International Telecommunication Union* (ITU)[11] publica anualmente el índice global de ciberseguridad (*Global Cybersecurity Index* o GCI), que mide el compromiso de los países en materia de ciberseguridad a nivel global. El índice se construye teniendo en cuenta el impacto de cinco pilares: (i) medidas legales; (ii) medidas técnicas; (iii) medidas organizacionales; (iv) desarrollo de capacidad; y (v) cooperación.

De acuerdo con el GCI publicado en 2023, usando información del año 2020, el Perú ocupa el lugar 86 de 182 países encuestados; mientras que, a nivel del continente americano, ocupa la posición 12

7 NIST, Information Technology Laboratory, Computer Security Resource Center, Glossary, en https://csrc.nist.gov/glossary/term/cybersecurity_risk

8 J. Elliott y N. Jenkinson, "El ciberriesgo es la nueva amenaza para la estabilidad financiera", en https://www.imf.org/es/Blogs/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability

9 Lagarde, Christine, "Estimación del riesgo cibernético en el sector financiero", en https://www.imf.org/es/Blogs/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector

10 Depository Trust & Clearing Corp (DTCC) (2020) y 12° encuesta anual de gestión de riesgos bancarios EY/IIF.

11 Agencia de Naciones Unidas especializada en tecnologías de la información y comunicación.

de un total de 35 países. Perú obtiene menores puntajes en los pilares "medidas organizacionales" y "desarrollo de capacidad", en tanto que el mayor puntaje obtenido corresponde a "medidas legales".

Por su parte, en Colombia, el Banco de la República ha elaborado el **indicador de riesgo cibernético** (IRC)[12], con información provista y recolectada por la firma de seguridad de la información *Security Scorecard*[13]. El IRC tiene una escala de cero a 100, donde un puntaje de 100 indica que no se detectaron problemas de ciberseguridad en el momento de la medición, y un puntaje de cero indica que se han detectado múltiples problemas que podrían comprometer la seguridad de la entidad financiera evaluada.

A partir del análisis del IRC para las entidades del sistema financiero de Colombia, el Banco de la República concluye que las cifras más recientes (a marzo de 2023) muestran que todos los factores utilizados para el cálculo del IRC tienen una calificación superior a 70 puntos, lo cual da cuenta de una buena administración del riesgo cibernético en el sistema financiero; aunque algunos indicadores (como seguridad de la red y *endpoint security)* podrían fortalecerse. En cuanto al IRC por tipo de entidad financiera, todas se ubican por encima de 80 puntos, lo que permite inferir que el sistema financiero ha tomado las medidas necesarias para protegerse ante vulnerabilidades cibernéticas.

Propuestas regulatorias sobre ciberseguridad a nivel internacional

A nivel internacional, las propuestas regulatorias en materia de ciberseguridad se enfocan en el **reporte de ciber incidentes** (*Cyber Incident Reporting* o CIR). Así, el Financial Stability Board (FSB), a solicitud del G20, preparó el documento "*Achieving Greater Convergence in Cyber Incidents Reporting*" (que se encuentra en consulta desde octubre de 2022), en el que se actualizan los términos y definiciones incluidos en el FSB *Cyber Lexicon,* con el objetivo de tener un lenguaje común y así lograr una mayor convergencia entre los CIR de distintas jurisdicciones. Asimismo, se presenta una propuesta de formato común del CIR entre jurisdicciones, que puede ser usado por las autoridades domésticas para recolectar información de ciber incidentes, así como para el intercambio de información con otras autoridades locales e internacionales.

Asimismo, el documento del FSB identifica algunos impedimentos para alcanzar una mayor armonización en el CIR y propone una serie de recomendaciones para superarlos, entre las que destacan:

i) Incentivar el acceso compartido a información, de manera que las entidades financieras compartan entre sí sus ciber incidentes y vulnerabilidades, así como conocimientos, a fin de estructurar una defensa colectiva del sistema financiero. Asimismo, se recomienda que las autoridades financieras y no financieras compartan información de ciberseguridad.

ii) Las autoridades financieras deberían tratar y procesar los CIR bajo ciertos principios, tales como el anonimato de los datos y restricciones para compartir los datos, a menos que la entidad financiera sea previamente notificada.

iii) Las autoridades financieras deben proporcionar *feedback* a las entidades financieras, a fin de fortalecer la ciber resiliencia del sistema financiero.

12 Ver Reporte de Estabilidad Financiera del Banco de la República de Colombia, I semestre de 2023.

13 Para la construcción del IRC se utilizan datos de diez factores o dimensiones del ciber riesgo, los cuales se agregan mediante un promedio ponderado, donde el peso de cada factor es determinado por *Security Scorecard,* utilizando técnicas de *machine learning*.

iv) Las autoridades financieras deben adoptar un enfoque constructivo antes que uno punitivo en el tratamiento de la información compartida, así como incentivar que las autoridades y entidades financieras compartan información relevante complementaria al CIR.

v) Las entidades financieras deben contar con protección legal, de modo tal que la información de los CIR no dé lugar a acciones legales, sanciones o a una mayor supervisión de estas entidades.

Regulación local en materia de ciberseguridad

El crecimiento de los canales digitales del sistema financiero, el cual se aceleró desde la pandemia, ha venido acompañado de riesgos relacionados a la ciberseguridad. Por ello, la SBS ha emitido normas sobre esta materia. Mediante Resolución SBS N° 504-2021 del 19 de febrero de 2023, la SBS aprobó el **Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad** (en adelante, el Reglamento), tomando en consideración la creciente interconectividad y mayor adopción de canales digitales para la provisión de servicios, así como la virtualización de algunos productos de los sistemas financiero, de seguros y de pensiones. El Reglamento establece normativa específica sobre gestión de seguridad de la información, complementaria al reglamento para la gestión del riesgo operacional, que toma en cuenta los estándares y buenas prácticas internacionales sobre seguridad de la información, entre los que se encuentran los del NIST y la familia de estándares de la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

En el Reglamento se define el **Sistema de Gestión de Seguridad de la Información y Ciberseguridad** (SGSI-C) como "el conjunto de políticas, procesos, procedimientos, roles y responsabilidades, diseñados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación ante incidentes de ciberseguridad". El SGSI-C implica, como mínimo, los siguientes principios:

i) Confidencialidad: la información sólo es disponible para entidades o procesos autorizados, incluyendo las medidas para proteger la información personal y la información propietaria.

ii) Disponibilidad: medidas para asegurar el acceso y uso oportuno de la información.

iii) Integridad: medidas para asegurar la autenticidad de la información y evitar su modificación o destrucción indebida.

Toda empresa que cuente con presencia en el ciberespacio debe mantener, con carácter permanente, un **Programa de Ciberseguridad** (PG-C) aplicable a las operaciones, procesos y activos de información. El PG-C debe prever un diagnóstico y plan de mejora sobre las capacidades de ciberseguridad, debiendo seleccionarse un marco de referencia internacional que permita, cuando menos, la identificación de los activos de información; la protección frente a las amenazas a los activos de información; la detección de incidentes de ciberseguridad; la respuesta con medidas que reduzcan el impacto de los incidentes; y la recuperación de las capacidades o servicios tecnológicos que pudieran ser afectados.

El Reglamento señala que la empresa debe reportar a la SBS, en cuanto advierta la ocurrencia de un incidente de ciberseguridad que presente un impacto adverso significativo verificado o presumible de pérdida o hurto de información de la empresa o de sus clientes; fraude interno o externo; impacto negativo en la imagen y reputación de la empresa; o interrupción de sus operaciones. Respecto al intercambio de información de ciberseguridad, se precisa que la empresa debe hacer los arreglos necesarios para contar con información que le permita tomar acción oportuna frente a las amenazas de ciberseguridad y el tratamiento de las vulnerabilidades (por ejemplo, suscribir acuerdos con otras empresas del sector o con terceros incumbentes, de forma bipartita, colectiva o gremial).