Recuadro 2: Indicador de riesgo cibernético

Mariana Escobar Villarraga
María Fernanda Meneses
Eduardo Yanquen*

La creciente digitalización de los servicios financieros ha aumentado la exposición del sistema a ataques cibernéticos, los cuales podrían comprometer la seguridad de la información, su operabilidad y, por ende, su estabilidad. La materialización de un evento de ciberriesgo que afecte el sistema de pagos puede interrumpir el flujo de las transacciones, lo que afectaría la confianza en el sistema y podría desencadenar eventos aún más graves para la estabilidad del sistema financiero, como por ejemplo corridas bancarias. Si bien actualmente la materialización de estos riesgos ha sido limitada, el continuo monitoreo y medición de la exposición de las entidades representa tanto un reto como una necesidad para las autoridades competentes tanto internacionales como locales.

Este recuadro presenta la metodología de cálculo del indicador de riesgo cibernético (IRC), el cual es uno de los indicadores monitoreados por el Banco de la República para medir este riesgo, y analiza sus resultados para las entidades que componen el sistema financiero colombiano con la información al 15 de marzo de 2023. En los próximos *Reportes de Estabilidad Financiera* se plantea incluir este indicador en los análisis de riesgo que enfrentan las entidades. El recuadro se divide en cuatro secciones: la primera presenta las perspectivas y materialización de algunos eventos recientes de riesgo cibernético y su seguimiento internacional y local; la segunda describe el IRC y su metodología de cálculo; la tercera presenta los datos y su análisis, y, finalmente, la cuarta corresponde a las conclusiones.

1. Monitoreo internacional y local del riesgo cibernético

Los eventos de materialización de riesgos cibernéticos han dejado ver la importancia de este asunto[1]. Ataques recientes a bancos centrales como el hackeo de la página web del Banco Central de Dinamarca en enero de este año (Reuters, 2023) y el ataque a más de treinta entidades gubernamentales de Costa Rica, incluido el Ministerio de Hacienda, en abril del 2022 llevó a tomar medidas a este último país, y así declarar el estado de emergencia. En este contexto, el Comité de Pagos e Infraestructura de Mercados (CPIM, por su sigla en inglés) y la International Organization of Securities Commissions (Iosco) (Central Banking, 2023) recientemente alertaron sobre vulnerabilidades en infraestructuras financieras claves en el ámbito global; además de los reportes publicados por la Junta de Estabilidad Financiera (FSB, por su sigla en inglés), el Fondo Monetario Internacional y el Banco de Pagos Internacionales (BIS, por su sigla en inglés).

Por lo anterior, el riesgo cibernético ha ganado importancia dentro del análisis del sistema financiero como un riesgo sistémico. En el nivel internacional, la encuesta *Barómetro de riesgo sistémico*, desarrollada e implementada por la Depository Trust and Clearing Corporation (DTCC, 2023), la cual recoge información de entidades estadounidenses y extranjeras, ubicó el riesgo cibernético como el tercero en importancia, al ser elegido por el 47,0 % de los encuestados como muy relevante para 2023[2]. Asimismo, la *Encuesta de riesgo sistémico* realizada por el Banco de Inglaterra en el primer semestre de 2023 ubicaba el riesgo cibernético en segundo lugar en importancia, después del riesgo geopolítico, al ser citado por 75,0 % de los encuestados como aquel que, de materializarse, sería de los más nocivos para el sistema financiero británico, y por el 9,7 % como su preocupación principal (Bank of England, 2023).

---

* Los autores son miembros del Departamento de Estabilidad Financiera (DEFI). Se agradece al Departamento de Seguridad Informática del Banco de la República y a Daniela Vargas, practicante del DEFI, por su apoyo en la elaboración de este recuadro.

1 Para el sistema financiero los principales riesgos relacionados con ciberseguridad comprenden: *ramsonware*, *malware*, ataques hacia plataformas web y *phishing*, entre otros.

2 El primer riesgo elegido por los encuestados como "muy relevante" fue el geopolítico junto con las tensiones comerciales, mientras que el segundo fue la inflación.

Adicionalmente, se han desarrollado indicadores, como el *global cybersecurity index* (GCI) publicado por la International Telecomunication Union (2023) de las Naciones Unidas, el cual presenta, por país miembro, las fortalezas y oportunidades de mejora en el monitoreo del riesgo cibernético. En el escalafón del GCI, Colombia se ubicó en el puesto 81 de 183 en el reporte más reciente, con datos a 2020[3].

En contraste, en el ámbito local, en los resultados de la *Encuesta de percepción sobre riesgos del sistema financiero*, desarrollada por el Banco de la República (2023), se ha observado un crecimiento en la cantidad de entidades que consideran el riesgo cibernético como uno de los cinco cuya materialización tendría mayor impacto sobre el sistema financiero[4]; sin embargo, su participación continúa siendo baja (2,8 % en la versión de diciembre de 2022). Adicionalmente, la afectación de los sistemas de información de una empresa del sector de la salud a finales del año pasado prendió las alarmas en el país.

Por su parte, la Superintendencia Financiera de Colombia (SFC) expidió la Circular Externa 007 de 2018 y la Circular Externa 033 de 2020 en las cuales, respectivamente, se imparten instrucciones sobre los requerimientos mínimos para la gestión del riesgo de ciberseguridad y se dictan los lineamientos para el reporte de métricas e incidentes relacionados con la seguridad de la información y la ciberseguridad. Adicionalmente, en enero de 2023 la SFC publicó el Recuadro "Medición de la madurez en la gestión del riesgo operativo en las entidades bancarias", en el cual analiza el nivel de madurez de las entidades frente a la adopción de políticas que combaten el riesgo cibernético. Además, la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria) cuenta con el Equipo de Respuesta a Incidentes de Seguridad (CSIRT, 2023), el cual se encarga de fomentar la colaboración de sus miembros y el intercambio de información para afrontar de manera efectiva las amenazas cibernéticas, además de brindar cursos periódicos de actualización.

2. Metodología de *scoring*

El IRC se calcula con información provista y recolectada por la firma Security Scorecard[5]. Para su construcción se utilizan datos de diez factores que representan diferentes dimensiones del ciberriesgo, los cuales se agregan mediante un promedio ponderado, donde el peso de cada factor es determinado por Security Scorecard utilizando técnicas de *machine learning* y se ilustran de forma categórica como *alta*, *media* y *baja* (Diagrama R2.1). El IRC tiene una escala de cero a cien, donde un puntaje de cien 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 evaluada.

3. Análisis del *score*

En su función de velar por la estabilidad del sistema financiero, el Banco de la República considera relevante monitorear las medidas que toman los establecimientos de crédito para protegerse frente al riesgo cibernético. Para conocer el nivel de protección de las entidades se utilizan los factores que componen el IRC y la calificación global del IRC dada por Security Scorecard. Al analizar la calificación de cada uno de los factores que componen el IRC, en el caso de los bancos se observa que los componentes que más variación presentan son el de *endpoint security* y el de *reputación IP*, siendo el primero el que menor calificación alcanza para este sector en noviembre de 2022 (Gráfico R2.1). Lo anterior significa que una proporción de los equipos que utilizan este tipo de entidades se encuentran expuestos y deberían someterse a chequeos de seguridad. Se destaca positivamente que factores como el *cubit score*, el *hacker chatter* y el de *seguridad de la red* presentan calificaciones excelentes durante todo el año. Sin embargo, llama la atención el comportamiento de factores como *patching cadence*, el cual ha venido disminuyendo consistentemente a lo largo del año y que

3 De acuerdo con la publicación (International Telecomunication Union, 2023), el país mostraba fortaleza en el indicador técnico, el cual mide la implementación de estrategias técnicas por medio de entidades nacionales y específicas por sector y oportunidades de mejora en el indicador organizacional, el cual mide las estrategias nacionales y a nivel de organización de ciberseguridad.

4 Los dos principales riesgos que mencionan las entidades en la encuesta son: deterioro en el panorama económico de Colombia y materialización del riesgo de crédito.

5 Security Scorecard es una empresa de seguridad de la información que califica las posturas de seguridad cibernética a través de análisis de amenazas con fines de gestión de terceros y gestión de riesgos de tecnologías de la información.

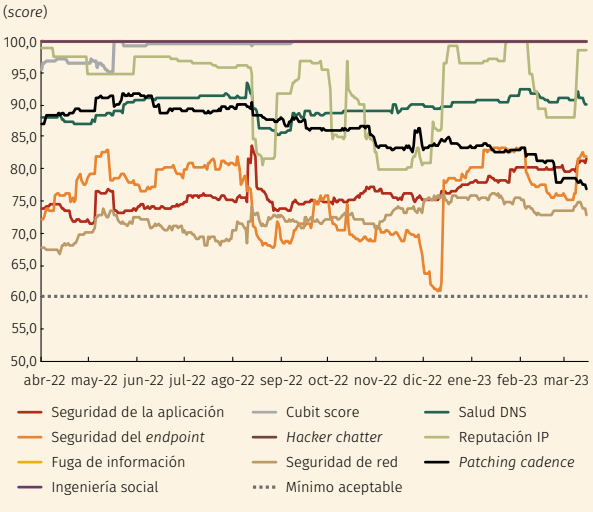
Diagrama R2.1
Módulos de indicadores de ciberseguridad

1. Reputación IP	Procesa millones de señales de *malware*[a/] y mapea direcciones IP infectadas	6. *Cubit scores*	Toma problemas críticos de seguridad y configuración, como paneles de control expuestos o IP vulnerables
2. *Endpoint security*	Mide metadatos relacionados con la seguridad de los equipos que la entidad tiene conectados a la red	7. *Hacker chatter*	Analiza conversaciones y mensajes clandestinos de piratas informáticos
3. Seguridad de la red	Cuantifica puertos abiertos, inseguros o mal configurados	8. *Patching cadence*	Mide la rapidez con la que una organización instala actualizaciones de seguridad
4. Seguridad de la aplicación	Analiza vulnerabilidades, configuraciones incorrectas y amenazas entrantes a través de aplicaciones web públicas	9. Fuga de información	Detecta credenciales expuestas a una violación de privacidad o filtración de información
5. Salud DNS	Valida que no ocurrieron eventos maliciosos cibernéticos	10. Ingeniería social	Mide la potencial susceptibilidad a un ataque en cuentas corporativas en redes sociales, cuentas financieras y listas de *marketing*

Ponderación: Alta Media Baja

a/ *Malware* es un término que designa cualquier *software* malicioso creado para dañar o aprovechar vulnerabilidades en las redes de información, servicios o dispositivos.
Siglas: *Domain Name System* (DNS) *Internet Protocol Address* (IP).
Fuente: *Security Scorecard*.

Gráfico R2.1
Factores de ciberseguridad de los bancos



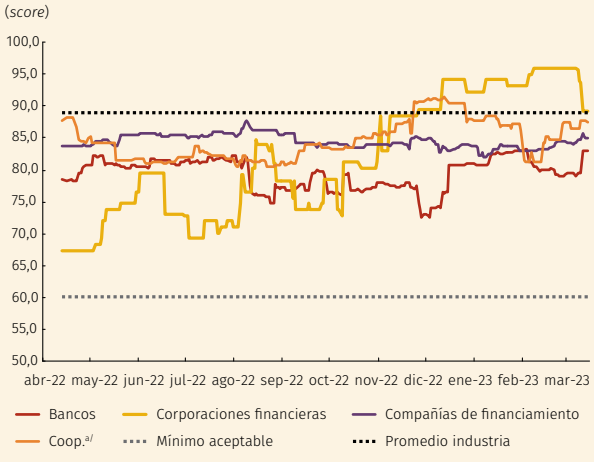
Fuente: *Security Scorecard*; cálculos del Banco de la República.

en las últimas mediciones se encuentra con una calificación de 76,8 puntos, siendo este el factor de más bajo desempeño luego de *seguridad de la red*, el cual se ubica en la última posición, con 72,9 puntos.

Para construir el IRC por tipo de entidad se tomó la calificación dada por Security Scorecard a cada una, se ponderó por su participación en el activo dentro de su grupo de referencia, y con estos datos se calculó el promedio. Para bancos y cooperativas se consideró el total de las entidades que componen estos grupos, mientras que para corporaciones financieras (CF) y compañías de financiamiento (CFC) se tuvo en cuenta a las entidades que representan el 92,4 % y el 78,9 % del activo, respectivamente, por disponibilidad de información.

En primer lugar, se observa que el IRC más volátil y, al mismo tiempo, el que ha tenido mayor mejoría durante el último año, al pasar de 67,4 a 89,2 puntos, es el que corresponde a las CF, el cual actualmente es el mejor entre los EC, aumento que ha estado impulsado, principalmente, por mejoras en los factores de seguridad del *endpoint* y salud DNS. Para los bancos y las cooperativas se han producido variaciones en su IRC, pero este se ha mantenido estable en el último año; sin embargo, es importante prestar atención a los factores con menor calificación para los bancos (Gráfico R2.2), pues este sector es actualmente el que registra el IRC más bajo del sistema. Por último, la calificación para las CFC ha permanecido relativamente estable en el último año. Estos datos se encuentran alrededor de la calificación promedio de la industria de servicios financieros que, según los da-

Gráfico R2.2
Promedio ponderado de la calificación por tipo de entidad



a/ Cooperativas financieras.
Fuente: *Security Scorecard*; cálculos del Banco de la República.

tos de Security Scorecard, para la fecha de corte se encontraba en 88 puntos.

4. Conclusiones

El monitoreo del riesgo cibernético continúa evolucionando y ganando importancia. En el nivel local, el IRC utilizado por el Banco de la República permite dimensionar el estado de las políticas y medidas implementadas por las entidades del sistema financiero colombiano. Las cifras más recientes del IRC muestran que todos los factores utilizados para su cálculo tienen una calificación superior a 70 puntos, lo cual da cuenta de una buena administración del riesgo cibernético para las entidades, en especial para las CF que han mejorado sus indicadores de manera significativa; sin embargo, indicadores como *seguridad de red* y *endpoint security* podrían fortalecerse. En cuando al IRC por tipo de entidad, todas se ubican por encima de 80 puntos, lo cual permite inferir que el sistema financiero ha tomado las medidas necesarias para protegerse ante vulnerabilidades cibernéticas.

Referencias

Banco de la República (2023). *Encuesta de percepción sobre riesgos del sistema financiero*, enero onsultado el 28 de abril de 2023 en https://repositorio.banrep.gov.co/handle/20.500.12134/10592

Bank of England (2023). "Systemic Risk Survey Results, 2023 H1", consultado el 28 de abril de 2023 en https://www.bankofengland.co.uk/systemic-risk-survey/2023/2023-h1

Central Banking (2023). "CPMI and IOSCO Raise 'Serious' Concern Over Cyber Security Flaw", consultado el 28 de abril de 2023 en https://www.centralbanking.com/central-banks/financial-stability/fmi/7953859/cpmi-and-iosco-raise-serious-concern-over-cyber-security-flaw

CSIRT (2023). "¿Quiénes Somos?", Asobancaria, consultado el 28 de abril de 2023 en https://csirtasobancaria.com/quienes-somos

DTCC (2023). "Systemic Risk Barometer Survey", consultado el 28 de abril de 2023 en https://www.dtcc.com/-/media/downloads/Systemic-Risk/Systemic-Risk-2023

International Telecommunication Union (2023). *GCI Fourth Edition Report*, consultado el 28 de abril de 2023 en https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Reuters (2023). "Hackers Hit Websites of Danish Central Bank, Other Banks", consultado el 28 de abril de 2023 en https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/