Evaluación de la Ciberseguridad en el Sistema Financiero Mexicano

Extracto del Reporte de Estabilidad Financiera – Diciembre de 2022, Recuadro 8, pp. 100 – 103. Documento publicado el 7 de diciembre de 2022.

1. Introducción

En este Recuadro se describen la metodología y resultados de los índices de ciberseguridad a los que le da seguimiento Banco de México, los cuales forman parte de las acciones que se llevan a cabo para evaluar y promover la ciberseguridad en el sistema financiero mexicano.

El sistema financiero ha aumentado su exposición al riesgo cibernético, el cual ha evolucionado de ser un riesgo operativo con un impacto limitado a ser considerado un riesgo para la estabilidad financiera y para la economía en general. En los últimos años, no solo se ha incrementado la importancia de las plataformas digitales y la adopción de esquemas de trabajo a distancia, sino que también ha aumentado la interconexión digital del sistema financiero. Las instituciones comparten activos, datos, software e infraestructura; lo que permite que un ciber ataque pueda rápidamente extenderse entre instituciones y poner en riesgo la estabilidad financiera, ya sea mediante pérdidas financieras o mediante la erosión de la confianza en el sistema.

El manejo del riesgo cibernético requiere una comunicación rápida y efectiva entre instituciones, y a su vez acciones en conjunto que permitan mitigar el riesgo. Con esto en mente, el Banco de México da seguimiento a índices internacionales como el Índice Global de Ciberseguridad (*GCI*) creado por la Unión Internacional de Telecomunicaciones (*ITU*),[1] que permite evaluar el estado de la ciberseguridad relativo a otros países. Sin embargo, debido a que la oportunidad de información es limitada,[2] también se han desarrollado herramientas que permiten un seguimiento constante del estado de la ciberseguridad en México. Entre estas herramientas están el Índice de Ciberseguridad de las Instituciones Financieras Reguladas por el Banco de México, el Índice de Percepción del Riesgo de Ciberataques al Sector Financiero y el Índice de Riesgo de Ciberataques en México.

2. Desarrollo de incidentes cibernéticos

El riesgo cibernético ha crecido de manera considerable derivado del aumento en las interconexiones y el creciente uso de tecnologías digitales. El sistema financiero no ha estado exento de estos desarrollos y el impacto de un ciberataque podría ser sistémico. Al respecto, la Junta Europea de Riesgo Sistémico (*ESRB*, por sus siglas en inglés) desarrolló un modelo conceptual para analizar las condiciones bajo las cuales un incidente cibernético podría constituir un riesgo sistémico. El modelo consta de 4 etapas:

1. Contexto: Circunstancias en las que ocurre un incidente cibernético. El análisis incluye el origen, las amenazas, las vulnerabilidades y los activos afectados.
2. Choque: Descripción del impacto inmediato del incidente para las instituciones afectadas, el impacto puede ser técnico (como perdida de confidencialidad) o de negocios (como pérdida de reputación).
3. Amplificación: Se divide en i) amplificadores que pueden aumentar el impacto o las consecuencias del choque y ii) mecanismos de transmisión (operacional, financiero o erosión de confianza).

[1] Véase sección V.5.2. Riesgos cibernéticos del Reporte de Estabilidad Financiera de junio 2022.
[2] El *GCI* se genera de manera bianual. Al momento de la publicación de este reporte, el índice más actualizado corresponde a datos del 2020.

4. Riesgo sistémico: Si se activan los mecanismos de transmisión el choque original puede transmitirse al sistema financiero y afectar instituciones que en un principio no fueron afectadas por el incidente cibernético.

Con el objetivo de mitigar los potenciales impactos de un ataque cibernético al sistema financiero, el Banco de México realiza un constante monitoreo en las diversas áreas que por su naturaleza pudieran ser susceptibles a un ciberataque. Asimismo, evalúa potenciales amenazas y se coordina con los participantes del sistema financiero con la finalidad de que desarrollen las herramientas necesarias para reducir los mecanismos y canales de amplificación de un ciberataque. Así, el Banco de México busca prevenir el desarrollo de un ciberataque que pudiera escalar para convertirse en un riesgo sistémico. Con esto en mente, se han desarrollado algunos índices que permiten dar seguimiento de manera constante y oportuna al tema de la ciberseguridad: i) al estado actual de sistema financiero en materia de ciberseguridad, ii) a la evolución de los ciberataques a nivel mundial y local y iii) a la potencial materialización de los ciberataques.

3. Índice de Ciberseguridad de las Instituciones Financieras Reguladas por Banco de México

Durante 2022, el Banco de México definió y construyó un índice para medir el estado de la ciberseguridad en las instituciones financieras reguladas por el Banco de México, es decir, identificar sus fortalezas y sus áreas de oportunidad.

Este índice se determina a través de un cuestionario de autoevaluación de 30 preguntas agrupadas en 5 temas:

Gobierno: Desarrollar una comprensión organizacional para administrar el riesgo de seguridad Cibernética.

La institución cuenta con una estructura de ciberseguridad que reporta a la alta dirección, cuenta con políticas de seguridad de la información y tiene identificados sus procesos críticos.

Capacidad Técnica: Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.

La institución cuenta con controles de seguridad de la información y realiza evaluaciones técnicas de seguridad para probar dichos controles.

Resiliencia: Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.

La institución cuenta con planes de respuesta a incidentes de ciberseguridad y de continuidad operativa y los prueba periódicamente.

Capacitación y Concientización: La institución tiene un programa de concientización en materia de ciberseguridad para todo el personal, y capacita al personal que opera o administra los controles de seguridad, así como a la alta dirección.

Inteligencia: Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.

La institución recaba información de inteligencia de amenazas y la analiza para, proactivamente, anticipar que algún riesgo asociado a ellas se materialice en su infraestructura o procesos.

Cada área recibe una ponderación del 20% y cada pregunta fue evaluada en una escala de 0 a 2. El puntaje máximo es de 60 puntos que equivale a un 100%. La autoevaluación fue respondida por 79 instituciones financieras reguladas por el Banco de México, y se alcanzó una calificación total ponderada del 82%.

Con base en estos resultados, destaca como fortaleza que las instituciones tienen bien identificados los procesos críticos del negocio, para protegerlos, y establecen políticas de ciberseguridad organizacional en las que incorporan la evaluación de los controles tecnológicos mediante pruebas de penetración (Pentest).

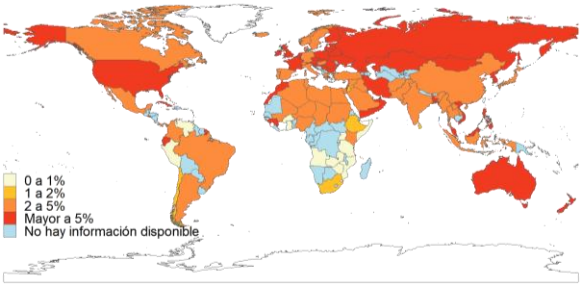
Asimismo, se identificaron áreas de oportunidad como: la necesidad de destinar personal especializado en el análisis y diseminación de información de inteligencia de amenazas que las instituciones ya recolectan; promover la capacitación en materia de ciberseguridad para la alta dirección y para las personas que operan procesos críticos de la entidad; y participar en ejercicios de ciberresiliencia que les ayuden a probar sus capacidades de detección, contención y respuesta, ante incidentes de ciberseguridad, individualmente o a nivel gremial.

Con base en los resultados de este ejercicio, Banco de México trabaja con las instituciones para atender las áreas de oportunidad identificadas mediante la autoevaluación.

4. Índice de Percepción del Riesgo de Ciberataques al Sector Financiero

Mide la percepción del riesgo cibernético en el sector financiero para distintos países con base en noticias de periódicos de cobertura internacional.[3] El índice por país se estima con base en una metodología desarrollada por el Fondo Monetario Internacional (FMI) y se calcula como la razón entre el número de noticias que se refieren al riesgo cibernético y el número de noticias que se refieren al riesgo en general, ambos tomando en cuenta solo el sector financiero,[4] por lo que entre mayor sea su valor existe mayor número de noticias de ciberataques financieros para el país evaluado. El Banco de México, al aplicar la metodología antes mencionada con noticias correspondientes al periodo de 2017 a 2022, encontró que México tiene una calificación de 4.36% y se ubica debajo de la media (6.81%) y la mediana (4.78%) del índice con respecto a todos los países, es decir está mejor en comparación con la mediana (Figura 1).

Figura 1
Índice de Percepción del Riesgo de Ciberataques al Sector Financiero



Cifras a noviembre 2022
Fuente: Banco de México con noticias de periódicos internacionales

[3] Reuters y cuentas oficiales de Twitter de periódicos internacionales: @Breaking views, @business, @markets, @BBCBusiness, @ftfinancenews, @MarketWatch, @BusinessInsider, @BW, @YahooFinance, @economics, @WSJmarkets, @CNBC, @financialpost.
[4] En el numerador está el número de noticias que contienen palabras relacionadas a ciberseguridad (cyber, cybersecurity), sector financiero (bank, market, financial, finance, insurance company, Fintech, credit card) y riesgo (risk, threat, vulnerability, uncertainty, loss, attack, incident, hack, fraud, data breach, data loss).

A partir del 2018, el índice observado para México ha mostrado una tendencia a la baja. A su vez, en los últimos tres años han disminuido las noticias que se refieren a riesgo cibernético en el sector financiero mexicano, lo que podría indicar una mejora en el estado de la ciberseguridad del sistema financiero mexicano.

Destacan los índices de Rusia y Estados Unidos, con valores mayores a 5%. Respecto a los Estados Unidos, el índice se encuentra actualmente en 6.72%, por encima de la mediana de la distribución de los países. A diferencia de México, el índice disminuye en 2019 y 2020 pero vuelve a aumentar en 2021; sin embargo, para 2022 se observa un nivel menor al 5%.

Por otro lado, Rusia acumula un índice de 10.6%, superior a la mediana de la distribución y cerca de duplicar la media. Aunque el índice presenta una disminución del 2021 al 2022, esto se debe a que si bien las noticias de ciber-riesgo aumentaron en un 15%, el denominador aumentó en 372%.

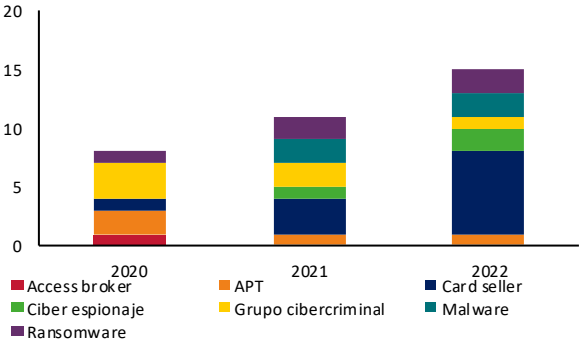
5. Índice de Riesgo de Ciberataques en México

Mide el riesgo cibernético en el sector financiero mexicano con base en fuentes de inteligencia de ciberseguridad. El índice representa el número de noticias en los que se mencionó una amenaza cibernética y que se comprobó un riesgo de ciberseguridad para el sector.

Gráfica 1[5]

Índice de Riesgo de Ciberataques en México

Número de noticias



Cifras a noviembre 2022

Fuente: Banco de México.

El año en el que se reportaron más noticias fue 2022, con 15. Los reportes de *ransomware* continúan aumentando y se mantienen como la mayor preocupación del sector financiero mexicano por su posible impacto

[5] **Access broker:** Actor de amenaza que accede ilegalmente a redes informáticas de organizaciones y revende los accesos a través de foros clandestinos de Internet.
APT: Amenaza Persistente Avanzada, por sus siglas en inglés, cuenta con altos niveles de especialidad en técnicas de hackeo y con los recursos y el tiempo que requiera para que, a través de la utilización de distintos vectores de ataque sofisticados, logre vulnerar a las organizaciones objetivo con el fin de sabotearlas u obtener información sensible o ganancias económicas.
Card seller: Actores de amenaza cuya principal actividad consiste en robar información relativa a tarjetas bancarias de los clientes de las instituciones financieras, con el fin de vender dicha información en foros clandestinos de Internet.
Ciber espionaje: Amenaza cuya finalidad es extraer información sensible de instituciones gubernamentales o de grandes corporaciones.
Grupo cibercriminal: Amenaza dedicada a realizar actividades delictivas dirigidas a sistemas informáticos principalmente con la finalidad de obtener recursos económicos. En esta categoría se agrupan las amenazas generalizadas que no se pueden asociar a alguna de las otras categorías.
Malware: Amenaza diseñada para comprometer la confidencialidad, integridad o disponibilidad de la información de un sistema informático.
Ransomware: Es un tipo de software malicioso cuyo fin es secuestrar información sensible de un sistema informático, a fin de que la víctima pague por el rescate de la misma o evite su publicación en foros clandestinos de Internet.

en la estabilidad financiera (Gráfica 1). Asimismo, continúan aumentando los reportes asociados a *Card sellers* quienes han identificado como un negocio lucrativo el robo y la venta de datos personales y financieros de los clientes de las instituciones financieras (por ejemplo, los datos de las tarjetas bancarias) en foros clandestinos de Internet. Si bien esto no representa una amenaza a la estabilidad financiera, sí genera un efecto desfavorable de largo plazo en la confianza que el público puede tener con las instituciones financieras durante el manejo de su información personal y el crecimiento de fraudes.

Las amenazas de los Grupos Cibercriminales generalizados han mostrado una tendencia a la baja que se explica como resultado de una diversificación y especialización de estos grupos en amenazas específicas como *ransomware*, *Card seller*, etc. A través de su Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información (GRI), las autoridades financieras han alertado de estos riesgos a las instituciones permitiéndoles aplicar medidas de prevención de incidentes.

6. Consideraciones finales

Banco de México promueve que las instituciones trabajen en robustecer su estrategia de ciberseguridad, madurando sus capacidades proactivas como son la inteligencia de amenazas, la concientización de todo su personal y alta dirección, y la práctica de simulacros de atención a ataques cibernéticos. Estas acciones, en conjunto con el cumplimiento de las medidas de ciberseguridad definidas en la regulación, dan paso a una mejor preparación para la defensa y resiliencia ante ciber incidentes. La alta interconexión del sistema financiero puede conducir a que la vulneración de una institución financiera afecte al sistema, por lo que es importante que las instituciones lleven a cabo esfuerzos para fortalecer aquellas áreas de ciberseguridad que así lo requieran.

El Banco de México realiza un monitoreo constante en materia de ciberseguridad desde distintas perspectivas. Asimismo, se mantiene una comunicación continua con las instituciones financieras en materia de coordinación y actualización asociadas a la evolución de los riesgos cibernéticos en el sistema, para de esta forma reducir la probabilidad de ocurrencia de un ciber incidente y mitigar su impacto, si llegara a ocurrir. Los índices presentados en este Recuadro fueron creados para desarrollar herramientas complementarias que nos permiten tener un diagnóstico del estado de la ciberseguridad en el sistema financiero mexicano. Aunque el diagnóstico es favorable, no se descarta que puedan existir riesgos cibernéticos que impacten de manera relevante al sistema financiero, por lo que la tarea de ciberseguridad es una actividad continua en la que se trabaja de manera constante para su mejora.

7. Referencias

International Telecommunication Union (2021): *"Global Cybersecurity Index 2020"*. Ver: Global Cybersecurity Index (itu.int).

Instituto Nacional de Estándares y Tecnología, "Marco para la mejora de la seguridad cibernética en infraestructuras críticas". [6] Versión 1.1, 16 de abril de 2018.

European Systemic Risk Board (2020): *Systemic cyber risk.* Ver: Systemic cyber risk (europa.eu)

Bouveret, A (2018): *"Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment",* WP/18/143, junio 2018

[6] Marco para la mejora de la seguridad cibernética en infraestructuras críticas (nist.gov).