8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Fitch Ratings

8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Factores Clave en la Evaluación de Riesgo Operativo

Especial énfasis en ciberseguridad

Fitch Ratings

8ª CONVENCIÓN AMS Asociación Mexicana de Sofipos

Riesgo Operativo - Ciberseguridad

- Relevancia de la Ciberseguridad
- Modelos de Negocio con + riesgo
- Tipos de ciberataques y pérdidas
- Mejores prácticas
- Aspectos Regulatorios
- Metodología Fitch

FitchRatings

8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Relevancia de la Ciberseguridad

Riesgo Impredecible

Relevancia de la Ciberseguridad

- La ciberseguridad cobró mayor relevancia con el COVID-19, que incrementó las actividades/transacciones y servicios financieros por medios digitales y la aplicación de prácticas de trabajo a distancia en la mayoría de las IFs.

- **Riesgo Impredecible:** Los ciberataques representan riesgo graves para las IFs, sin embargo, estos son impredecibles y pueden tener efectos adversos financieros, reputacionales y operativos. No solo sobre emisores individuales, sino también en sistemas financieros en un sentido más amplio.

- Banco de México (Banxico) indica que en años recientes se ha observado a nivel global un aumento constante de ciberataques al sector financiero. Principalmente a instituciones bancarias, bancos centrales y sistemas de pagos para operaciones internacionales (debido a su mayor automatización, complejidad de procesos y nivel de recursos adinistrados).

Relevancia de la Ciberseguridad

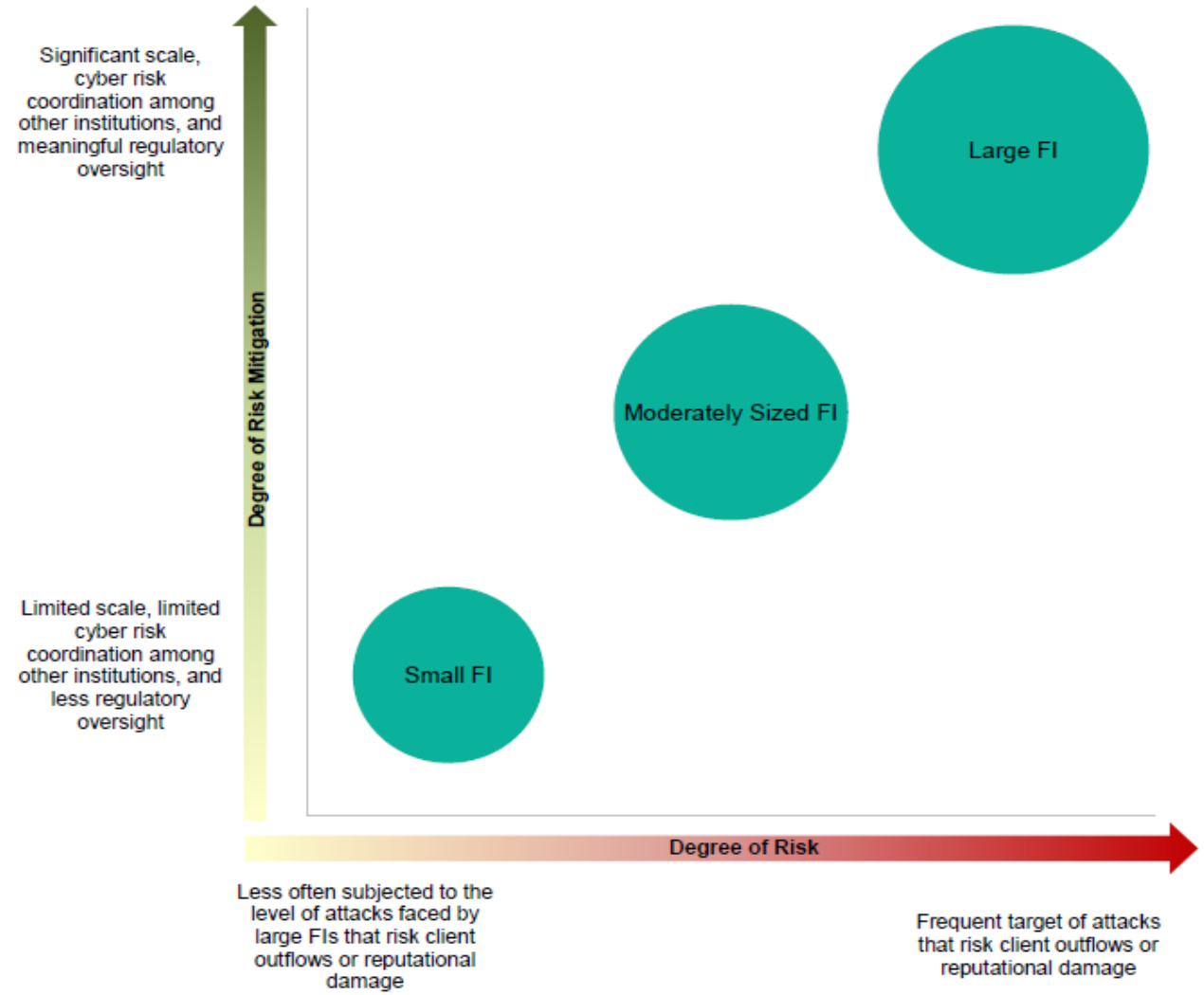
- **Posición de Mercado:** Cuanto más grandes sean los negocios de banca de consumo y la franquicia de depósitos de una institución financiera, mayor será la amenaza de ataques porque tienen datos de clientes más sensibles y valiosos. Por lo tanto, Fitch considera que la exposición en la banca comercial es mayor.

- No obstante, las IFNB no están exentas a este riesgo operacional y en algunos casos las IFNBs tienden a priorizar rentabilidad y dejar en segundo plano inversiones en el fortalecimiento de seguridad cibernética.

- **Equilibrio entre innovación y seguridad:** las IFs se esfuerzan por lograr un equilibrio al ofrecer productos y servicios innovadores a sus clientes, la mejor experiencia para el cliente y seguridad, incluida la ciberseguridad. Las IFs corren el riesgo de degradar la experiencia del cliente si la seguridad es demasiado onerosa.

Risk Factors and Mitigation

Overview of Institution Size Exposure to Cyber Risk
(High and Elevated Risk Institutions)



Source: Fitch.

Fitch Ratings

8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Modelos de Negocio con Mayor Riesgo

Modelos de Negocio con Mayor Riesgo

- Las IF con frecuencia han experimentado intentos de ciberataques, motivado por obtener una ganancia financiera o provocar una interrupción de la infraestructura financiera, o una combinación de ambas.

- Actividades empresariales como banca de consumo/préstamos y comercio minorista, los servicios de corretaje están relativamente más expuestos a ser objeto de ataques , dado que poseen información valiosa y sensible de clientes.

- Los modelos de negocio enfocados a la ejecución, compensación y liquidación de valores, podría ser propenso a ataques motivados por ataques disruptivos que interfieran con la interconectividad con el sistema financiero.

- Dicho esto, las IF más grandes y de alto riesgo tienden a tener mejores controles de riesgo y escala para mitigar ataques cibernéticos.

- Colaboraciones / Alianzas: las alianzas con empresas de tecnología o con plataformas de pago también están expuestas, pues los ataques también pueden darse en el socio.

Overview of Business Activity Exposure to Cyber Risk

	Financially Motivated Cyber Risk	Crossover (Elements of Both)	Disruptively Motivated Cyber Risk
High Risk	Consumer Lending and Leasing and Investment Services (Consumer Fincos, Retail Brokers)	Substantial Commercial and Consumer Banking with Current/Checking Accounts (GSIBs)	Exchange, Clearing and Settlement Services (FMIs)
Elevated Risk	Asset Management Services (Investment Managers, Wealth Managers, Mortgage Servicers)	Securities Trading, Commercial Banking (Broker-Dealers, Large Regional Banks)	Sovereign Sponsored Financial Services Organizations (GSEs)
Moderate Risk	Commercial Lending and Leasing and Niche Institutions (Equipment Lessors, BDCs, Community Banks)	Financial Market Intermediaries (IDBs)	Not Applicable

FitchRatings

GSIBs – Global systemically important banks. FMIs – Financial market infrastructures. GSEs – Government-sponsored enterprises. BDCs – Business development companies. IDBs – Inter-dealer brokers. Source: Fitch.
Exposure refers to likelihood and frequency of attacks or the relative lucrativeness of targets for attackers. Exposure does not address the relative resilience of entities if an attack occurs, which is likely to be lower for

8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Tipos de Ciberataques

Potenciales pérdidas

Definición y tipos de ciberataques

- **Definición de riesgo cibernético:** Fitch no considera la definición más amplia de riesgos tecnológicos, como las relaciones de las IF con los proveedores de hardware, la velocidad del software de los sistemas o la ubicación geográfica de los centros de datos, como riesgos cibernéticos.

- Los riesgos cibernéticos analizados desde nuestra metodología se relacionan más con:

  - Interrupciones deliberadas de las plataformas o páginas web de las IF.
  - Que los datos de clientes se vean comprometidos.
  - Disrupciones de la infraestructura financiera.

- **Tipos de ataques cibernéticos**
  - Denegación de Servicio (DoS por su definición en ingles)
  - Amenaza Avanzada Persistente
  - Phishing
  - Malware
  - Caballo de Troya
  - Virus
  - Spam
  - Suplantación de identidad

Potenciales Pérdidas

- **Pérdidas monetarias** (el monto varía dependiendo del tamaño de la institución) por daños a la reputación que podría provocar salidas de clientes y/o pérdida de la confianza de los inversionistas.

- **Seguro contra Ciberataques** – podría cubrir de manera manejable pérdidas nominales pero puede no contener daño reputacional.

- Con base a información del equipo de seguros de Fitch en EE.UU., las primas emitidas directas de seguros cibernéticos para la industria de propiedad y accidentes (P/C) crecieron un 51% en 2022 a más de USD7.2 mil millones, según los datos financieros legales incluidos en el Suplemento de Cobertura de Seguro de Ciberseguridad y Robo de Identidad.

8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Mejores Prácticas

Infraestructuras de Riesgos

Mejores Prácticas

Existen marcos de mejores prácticas en la industria del riesgo cibernético que las IF y sus equipos directivos podrían elegir emplear.

Ejemplos

La firma de contabilidad PWC ha recomendado que los equipos directivos tomen en cuenta los siguientes aspectos:

- Establezcan la gobernanza del riesgo cibernético
- Comprendan los límites del riesgo cibernético en sus organizaciones
- Identifiquen procesos y activos críticos del negocio
- Identificar amenazas cibernéticas
- Mejorar o establecer un proceso de recopilación, análisis y reporteo de información.
- Formular planes para responder a los ciberataques.

Mejores Prácticas

Ejemplos

La consultora Oliver Wyman ha propuesto en términos generales un marco de gestión de riesgo cibernético que las empresas de servicios financieros deben emplear. (https://www.oliverwyman.com/our-expertise/insights/2017/jun/cyber-risk-management.html)

Banxico en conjunto con otras autoridades financieras elaboró una estrategia de mitigación de riesgos cibernéticos basada en tres pilares fundamentales:

- Gobierno Coporativo con importancia elevada en seguridad de la información
- Fortalecimiento preventivo de sistemas e infraestructura (con la aplicación de mejores prácticas, esquemas de gestión de riesgos institucional, desarrollo de equipos de trabajo y protocolos para la respuesta a incidentes).
- Una recuperación oportuna de la organización ante los posibles ciberataques

Mejores Prácticas

- Fitch no tiene un sesgo hacia un marco de gestión particular.
- Nuestro análisis se centra sobre si existe o no una estructura integral en vigor que ayuda a identificar, guiar y mitigar los controles de riesgo del emisor, y qué sea acorde a su modelo de negocios.
- Por razones de seguridad hay ciertas entidades en el sistema financiero mexicano que controlan estrictamente la divulgación pública sobre sus estrategias y tácticas para abordar las amenazas cibernéticas.

Infraestructura de Riesgos

- La capacidad de una IF para identificar, medir, gestionar y monitorear el riesgo a menudo está dictada por sus sistemas y controles de riesgo, por lo que la inversión continua en tecnología es fundamental.

- Es posible que las entidades pequeñas con presupuestos limitados o plataformas rudimentarias necesiten subcontratar algunas o la mayoría de sus funciones de ciberseguridad.

- El tamaño y la posición en el mercado también contextualizan la vulnerabilidad a los ciberataques. Por ejemplo, un banco minorista en un mercado desarrollado estará dispuesto a tolerar una mayor exposición al riesgo cibernético (e intentará mitigarlo) porque necesita innovación y nuevas formas de interactuar con los clientes para que su negocio sea competitivo a largo plazo.

8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Aspectos Regulatorios

Aspectos Regulatorios en México

- En los últimos 5 años se han implementado regulaciones en los sectores bancario y Fintechs: el requerimiento de un Oficial en Jefe de Seguridad de la Información que sea responsable de la estrategia institucional de seguridad de la información.

- Entre las entidades reguladas que conforman el sistema financiero, se exhiben disparidades en los requerimientos regulatorios en materia de seguridad de la información y de infraestructura tecnológica que aplica a cada tipo de entidad. L
- Las instituciones de banca múltiple y las Fintech poseen una regulación más estricta, seguidas por las casas de bolsa.

- Dichas regulaciones, son mucho más detalladas que las de otras instituciones financieras no bancarias siendo la regulación de las Sofomes la que presenta un menor detalle.

Aspectos Regulatorios Relevantes

- En su reporte de 2022, la CNBV expresó que en ese año realizó un análisis de la regulación existente para identificar áreas de mejora y garantizar que todos los integrantes del sector financiero mexicano cuenten con un marco regulatorio homologado.

- Se está desarrollando una propuesta de circular (Circular única de ciberseguridad) que integra y sistematiza las disposiciones en materia de seguridad de la información, mismas que serían aplicables a todas las entidades financieras que supervisa la CNBV (incluyendo Sofipos).

- La circular considera los principios mínimos necesarios para la mitigación de los riesgos cibernéticos, los mecanismos relevantes para procurar la seguridad de las operaciones y la salvaguarda del patrimonio de los clientes en las transacciones financieras digitales.

8ª CONVENCIÓN

Asociación Mexicana de Sofipos

Metodología Fitch

Fitch Ratings

Aplicación Metodológica

- Como parte de nuestro análisis para IFNBs incorporamos temas de riesgo operativo y ciberseguridad, dentro del factor de **Perfil de Riesgos**. La evaluación es cualitativa.

- Dentro de este factor se analiza lo siguiente:

  - Cómo es la gestión de riesgos en la institución.
  - Límites empleados
  - Herramientas y modelos para mitigar distintos tipos de riesgos
  - Otros aspectos.

Hallazgos

- No se han presentado impactos económicos u operativos en los últimos 12 meses como resultado de un ciberataque.

- Implementación de desarrollos tecnológicos o reforzamiento de procesos:
  - la realización de capacitaciones a todo el personal para concientizar sobre este tema
  - reforzamiento y actualización de procesos, herramientas
  - mayor inversión para el desarrollo tecnológico en la mayoría de las entidades

- Pruebas periódicas para la detección y corrección de vulnerabilidades.

- Pocas entidades cuenta con seguros que cubran el riesgo cibernético.

- Fitch percibe que las IFNBs presentan una menor exposición a este tipo de riesgo, aunque conforme continúen con la aplicación de canales digitales hacia sus clientes, este riesgo cobrará más importancia al igual que en el sector bancario.

Consideraciones Finales

La transformación hacia productos y servicios digitales es inminente y necesaria como herramienta para el avance en la inclusión financiera en México.

Dicha transformación se espera que vaya de la mano de una gestión proactiva y dinámica de los riesgos cibernéticos.

Lo anterior podría desarrollarse de manera más ágil mediante la guía de una regulación más detallada y estandarizada entre los distintos sectores, así como la adopción de mejores prácticas en las entidades no reguladas.

Gracias por su atención!

FitchRatings