Ciberseguridad en la Industria Bancaria

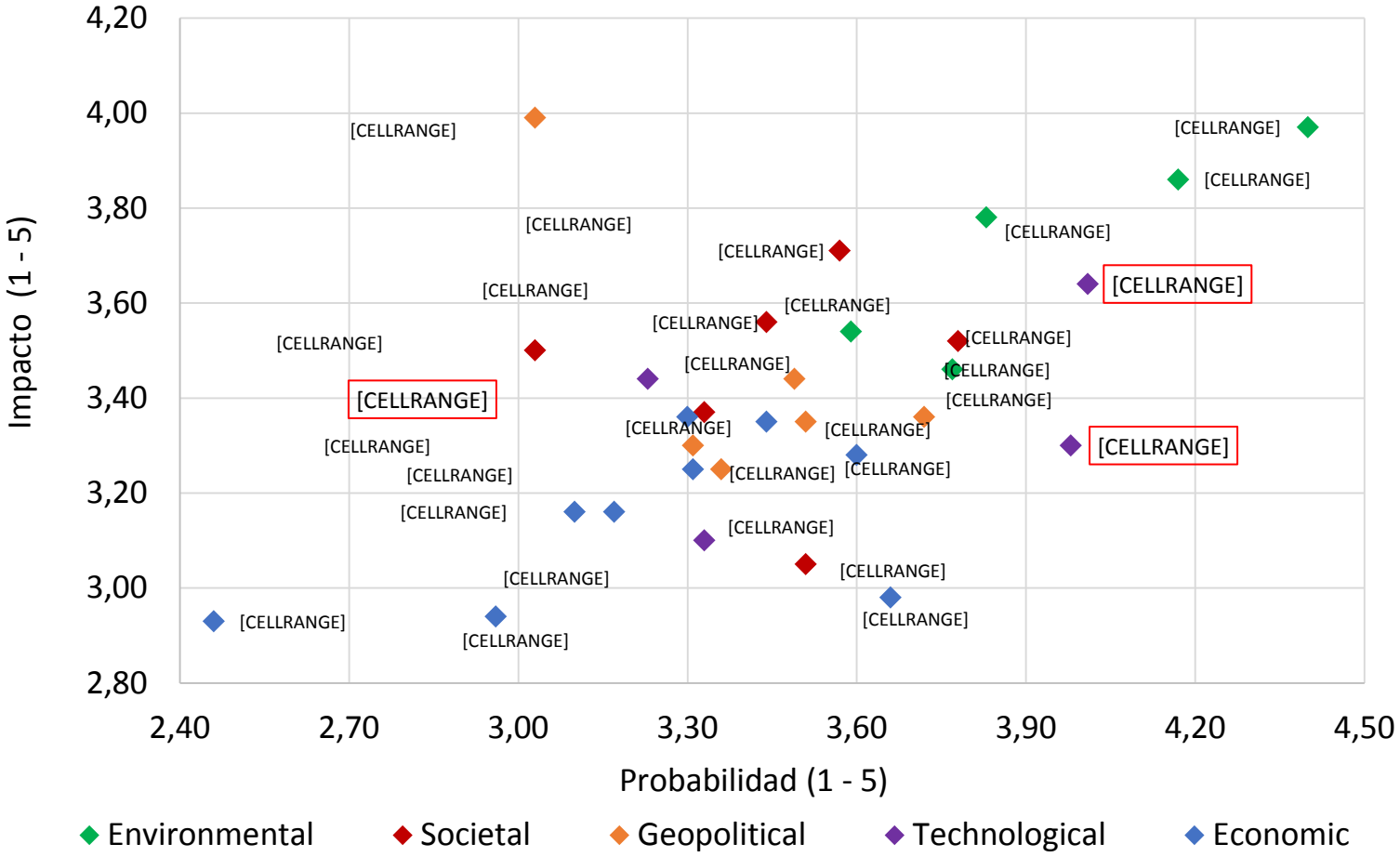
Segismundo Schulin-Zeuthen
Presidente
Asociación de Bancos

Junio 2018

Ciberseguridad: Precoupación para todos los sectores a nivel global

Mapa de Riesgos 2018

Impacto y probabilidad de ocurrencia de riesgos en el mundo [1]



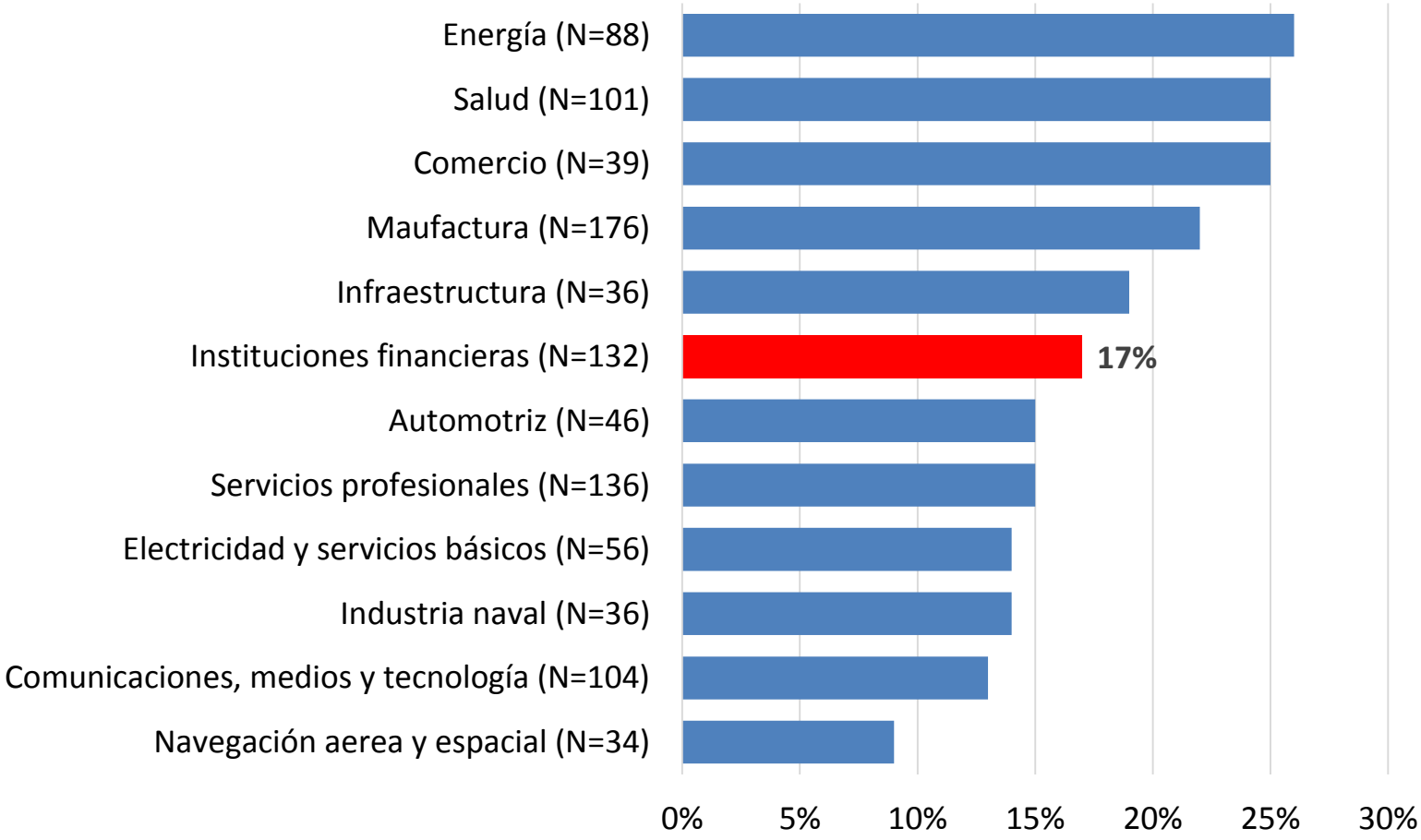
Fuente: World Economic Forum, The Global Risks Report 2018.

[1] Los encuestados evaluaron la probabilidad de ocurrencia de cada riesgo global en una escala de 1 a 5, donde 1 representa un riesgo que es muy improbable y 5 un riesgo que es muy probable de ocurrir. También evaluaron el impacto de cada riesgo global en una escala de 1 a 5 (1: impacto mínimo, 2: impacto menor, 3: impacto moderado, 4: impacto severo, 5: impacto catastrófico).

El sector financiero, si bien no es el objetivo más frecuente de ciberataques, enfrenta una amenaza importante en ciberseguridad a nivel global

banca
asociación de bancos

Industrias afectadas por ciberataques en 2017
(Porcentaje de empresas por que han sufrido ciberataques)



Fuente: Microsoft Global Cyber Risk Perception Survey. Encuesta a cerca de 1.000 altos ejecutivos en diferentes industrias)

Ciberseguridad: También es una preocupación en Chile

- El marco regulatorio pone especial énfasis en este tema
  - SBIF –normativa especifica a Ciberseguridad
  - Banco Central de Chile – medios de pago
  - Ley de Bancos –cargo de capital por riesgo operacional y Pilar II
- La banca también ha impulsado diversas medidas de prevención y mitigación frente a potenciales amenazas en ciberseguridad

Normativa SBIF

- La SBIF actualizó en enero 2018 sus requerimientos en materia de ciberseguridad
  - Incorpora el área de ciberseguridad explícitamente en la gestión de riesgo operacional, incluyendo equipos dedicados, realización de pruebas periódicas, involucramiento del Directorio y planes de contingencia, entre otros.
  - Establece el requisito de informar a la SBIF los incidentes relevantes, y además establece las condiciones de una base de incidentes en el ámbito de la ciberseguridad.
  - Explicita ciberseguridad como una materia dentro de los Lineamientos de Educación Financiera de la banca.
- En general, ***la normativa chilena no presenta brechas relevantes con los estándares internacionales***.

Normativa del Banco Central de Chile

- El Banco Central en junio de 2017 perfeccionó la normativa aplicable a los emisores de tarjetas de pago (Tarjetas de Crédito, Tarjetas de Débito y Tarjetas de Pago con Provisión de Fondos), conteniendo requisitos específicos en riesgo y ciberseguridad, entre ellos se encuentran los siguientes:

  - Emisores deben contar con **resguardos operacionales y de seguridad**, conforme a los estándares y mejores prácticas internacionales sobre medios de pago.

  - Deben contar con **tecnología de seguridad** que asegure la información contenida en las tarjetas, implementar mecanismos robustos de autentificación y **prevención de fraudes**.

  - Emisores deben establecer **políticas de gestión y control de riesgos operacionales, tecnológicos y de fraude, aprobadas por el directorio** (continuidad operacional, medidas de ciberseguridad para prevenir y mitigar los riesgos de fraude).

Ley de Bancos

- El proyecto de ley que moderniza la regulación bancaria introduce modificaciones a la Ley General de Bancos que guardan relación directa con el riesgo operacional en general, y por ende en temas de ciberseguridad, a saber:

  - La CMF establecerá mediante norma de carácter general, previo acuerdo favorable del Consejo del Banco Central, metodologías estandarizadas para **requerir capital por concepto de riesgo operacional**.

  - La CMF podrá imponer requerimientos patrimoniales adicionales a los bancos que, como resultado del proceso de supervisión, presenten, a juicio de la Comisión, riesgos no suficientemente cubiertos, incluyendo al **riesgo operacional,** hasta por 4% de sus activos ponderados por riesgo.

- En consecuencia, la aprobación del proyecto de ley no solo permitirá actualizar de manera general el marco regulatorio chileno, sino también aborda explícitamente la gestión de riesgos, dentro de la cual se encuentra la ciberseguridad.

Puntos Principales Marco Regulatorio

- En síntesis, existe un marco regulatorio en ciberseguridad específico para la industria bancaria
- Este marco regulatorio debe ser fortalecido, destacando lo siguiente:
  - **Aprobación del Proyecto que moderniza la Ley de Bancos**.
  - **Fortalecimiento presupuestario** del regulador bancario para una efectiva supervisión.
  - **Perímetro regulatorio**. La ciberseguridad tiene un carácter sistémico e involucra a diversos agentes financieros regulados y no regulados que debieran cumplir los estándares de seguridad equivalentes a la banca.
  - **Información y coordinación son claves**. La ciberseguridad es una materia que afecta distintos actores (incluyendo proveedores).
  - **Sistema de pagos**. El funcionamiento del sistema de pagos es critico e involucra a bancos y otros agentes (por ejemplo, camáras, AFPs, LBTR, etc.), por ende se requiere una aproximación sistémica en mitigación de riesgo y planes de contingencia.
- **La sobre-regulación a través de enfoques demasiado prescriptivos no es la solución**, y puede ser perjudicial por el dinamismo propio de la ciberserguridad (BIS, 2017).

Puntos Principales Marco Regulatorio

- El tema de ciberseguridad **no es un tema exclusivo de los bancos**, y tiene un importante componente de **extraterritorialidad**.

- La naturaleza transfronteriza de las amenazas de ciberseguridad requiere un **alineamiento de los marcos regulatorios** y **cooperación entre jurisidicciones para la detección y sanción de los ciber-crimenes.**

- Este alineamiento y cooperación, por lo expuesto previamente, debe ser liderado a **nivel país** tomando como base la Política Nacional de Ciberseguridad presentada el año recién pasado.

- La Política Nacional de ciberseguridad contiene lineamientos generales y objetivos de política para el año 2022.

- La implementación efectiva de dichos lineamientos y objetivos será complejo, pero es imperativo realizarlo en el corto plazo, donde se requerirá la revisión de tipos penales y sanciones para delitos informáticos, cooperación internacional para el intercambio de información y la detección y sanción de cibercriminales.

La Asociación de Bancos y Ciberseguridad

- En materia de prevención de fraudes, y ciberseguridad en general, los bancos individualmente realizan constantes inversiones y desarrollos, sin perjuicio de las iniciativas gremiales.
- **La Asociación ha implementando una institucionalidad para abordar específicamente los desafíos de ciberseguridad**.

I. Comité de Ciberseguridad de la Banca

- El 2017 se creó un Comité de Ciberseguridad siguiendo los lineamientos internacionales, integrado por todos los bancos.
- El objetivo es compartir información de amenazas potenciales y ataques de ciberseguridad, y coordinar acciones de mitigación.
- En los eventos recientes, este Comité funcionó según los protocolos y reglamentos establecidos, siendo una valiosa fuente de información para la industria.
- La existencia de este Comité también permitió comunicar oportuna y verazmente al público el alcance acotado del último evento.

- En este sentido, la **institucionalidad** en materia de ciberseguridad de la Asociación fue un valioso aporte para **preservar el funcionamiento del sistema de pagos y la confianza de los clientes**.

La Asociación de Bancos y Ciberseguridad

- En materia de fortalecimiento de la seguridad de los servicios y productos bancarios, entre ellos se destacan los siguientes:

  - El Directorio de la ABIF acordó que para fortalecer el estándar de seguridad de los medios de pago a contar del 1 de abril de 2017 sus miembros **solo emitirían tarjetas de crédito y débito que incorporen chip.**
  - El Comité de Gerentes Generales acordó que el flujo de cajeros instalados a partir del 1 de enero de 2018 constasen con **perturbador magnético**, incorporándose al stock total de cajeros esta tecnología el 1 de julio 2018.
  - La Asociación presentará una **propuesta en materia de TEF** (instantaneidad) que equilibra la seguridad de los clientes y la banca con la prestación de los servicios contratados.
  - La banca ha adoptado estándares de **comunicación de las operaciones a sus clientes**, donde los bancos informan a sus clientes las TEF.
  - Protocolo para **compartir información** agregada de fraudes. Informe mensual con cifras agregadas de fraude, es útil para alertar sobre desarrollos recientes a nivel de industria.
  - Campañas de **educación financiera a los clientes**, donde se enfatizan conceptos claves como cuidar la clave, entrar directo al sitio del banco y no a través de links, no responder a emails que piden información de claves y *passwords*, etc.
  - Determinación de **proveedores críticos**, evaluaciones y auditorías de ciberseguridad

Conclusiones

- Existe un marco regulatorio en materia de ciberseguridad
- La ciberseguridad es un tema prioritario para la banca y la Asociación de Bancos
- Es clave contar con información y la coordinación con los reguladores, dado el impacto sistémico que puede tener un evento de ciberseguridad
- El desafío en ciberseguridad es permanente, tanto para el sector público como privado (y no solo en bancos).
- En este sentido, es importante fortalecer los mecanismos para mitigar la ocurrencia de ciberataques y, además, perfeccionar la institucionalidad (organización, protocolos, etc.) destinada a aumentar la resiliencia del sistema financiero.
- El objetivo de estas acciones siempre debe ser mitigar los efectos en la **prestación de servicios a clientes**, **el normal funcionamiento del sistema de pago**s y **la estabilidad financiera**.

Ciberseguridad en la Industria Bancaria

Segismundo Schulin-Zeuthen
Presidente
Asociación de Bancos

Junio 2018