Superintendencia de Bancos e Instituciones Financieras Chile

Ciberseguridad en la Industria Financiera

Eric Parrado H. (@eric_parrado)
Superintendente de Bancos e Instituciones Financieras

15 de marzo de 2017
RBECA Liquidnexus

Strategic priorities for banks

Management's agenda remains dominated by risk and regulation. Their top four priorities are:

1. Managing reputational risk, including conduct and culture risks
2. Meeting regulatory compliance and reporting standards
3. Enhancing cyber/data security
4. Meeting capital, liquidity and leverage ratio requirements

Globalmente, los costos del cibercrimen son significativos...

- **US$575.000 millones (0,5% del PIB global)** es lo que el cibercrimen le cuesta al año al mundo (CSIS - McAfee, 2014).

- **US$90.000 millones (1,2% del PIB de la región)** al año es el costo para América Latina y el Caribe (Prandini et al 2011).

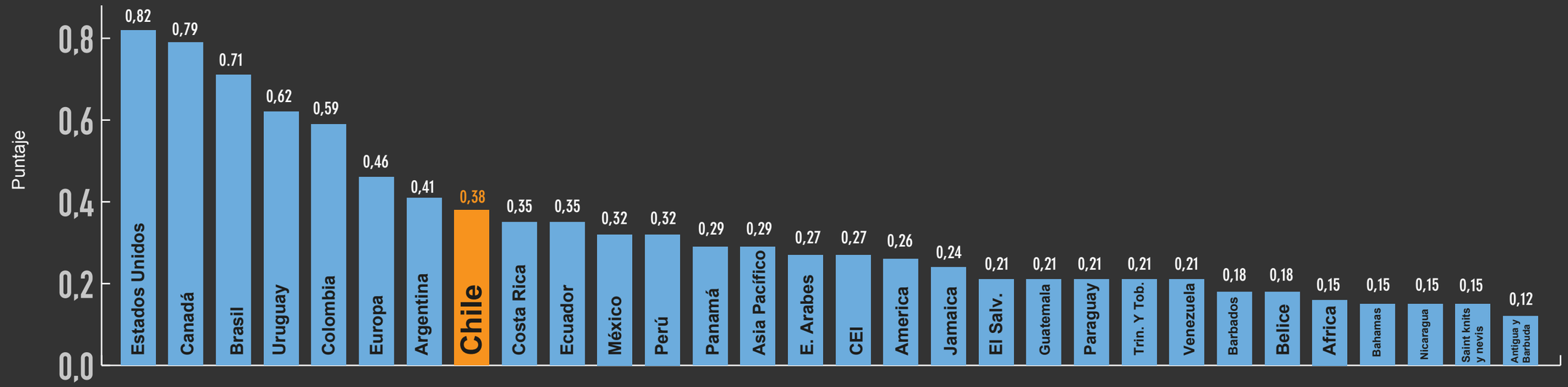
- **Estos costos aumentan entre 20% - 40% anualmente** (Ponemon Institute, 2016). En 2016 Brasil, Australia y Japón presentaron los mayores aumentos en los costos asociados a cibercrimen (37%, 24% y 23% respectivamente).

Superintendencia de Bancos e Instituciones Financieras Chile

La última evaluación de la Unión Internacional de Telecomunicaciones sitúa a Chile en la posición 16 (mejor preparado) de 195 países a nivel mundial y 7 a nivel regional

El índice no pretende determinar la eficacia ni el éxito de una medida adoptada, sino simplemente la existencia de estructuras nacionales para implementar y promover la ciberseguridad.

Índice Mundial de Ciberseguridad
(agrupaciones y países latinoamericanos)



Nota: El índice varia entre cero (peor preparación) y uno (mejor preparación), para una evaluación de 34 indicadores asociados a cinco ámbitos: jurídico, técnico, organizativo, creación de capacidades y cooperación internacional. Fuente: UIT (2015).

La mayoría de los países de la región (América Latina y el Caribe) están poco preparados para contrarrestar la amenaza del cibercrimen

- Falta de madurez en materias de ciberseguridad:
  - Cuatro de cada cinco países no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica.
  - Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética.
  - La gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos.

- Chile se encuentra en la mayoría de las categorías entre la segunda y la tercera etapa de desarrollo (de un total de cinco).

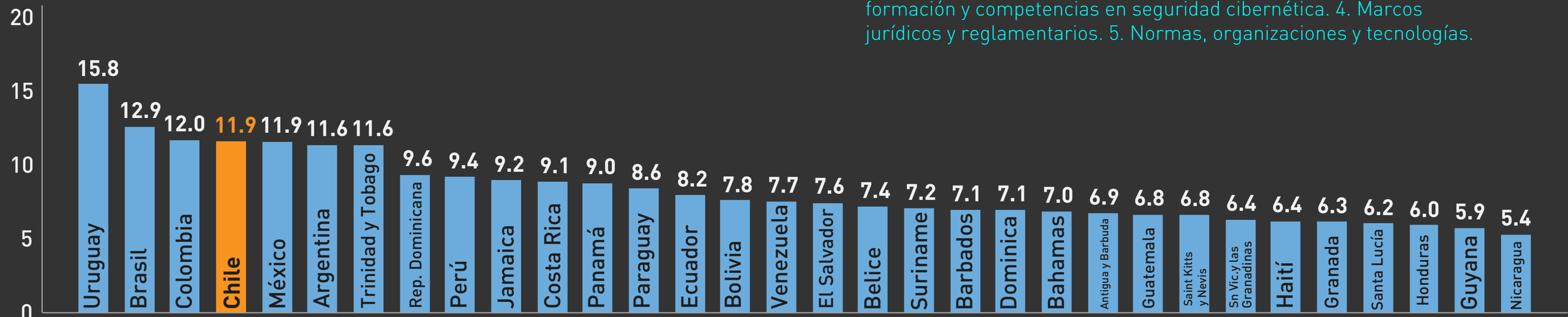
- Para avanzar, está pendiente la definición de una infraestructura crítica nacional compuesta y protegida por asociaciones público-privadas que permitan actuar en conjunto frente a eventuales ataques, con roles y responsabilidades bien definidas, manteniendo el equilibrio entre tecnología, innovación, gestión de riesgos y la continuidad de los distintos sistemas.

Superintendencia de Bancos e Instituciones Financieras Chile

Chile ocuparía la cuarta posición en madurez cibernética entre los países de la región (América Latina y el Caribe)

Usando los indicadores del estudio BID-OEA (2016), Chile está cuarto en la región. Su puntaje (11,9 de 25) lo califica con un nivel de madurez cibernética limitada.

El informe evalúa cinco dimensiones: 1. Política y estrategia de seguridad cibernética. 2. Cultura y sociedad cibernética. 3. Educación, formación y competencias en seguridad cibernética. 4. Marcos jurídicos y reglamentarios. 5. Normas, organizaciones y tecnologías.



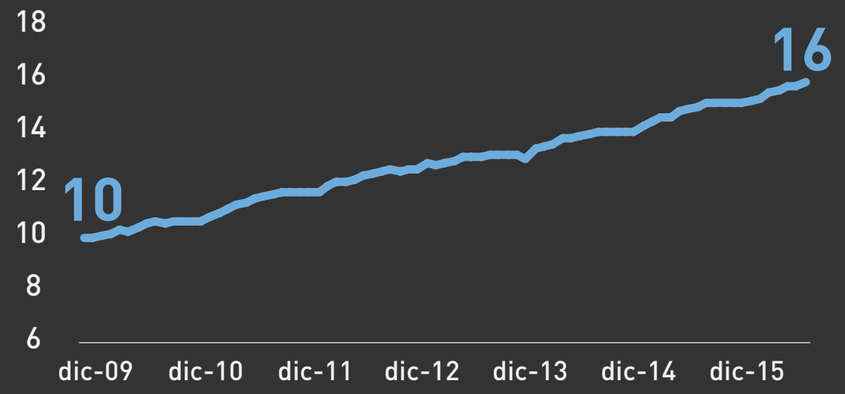
Fuente: Elaboración propia sobre la base de BID-OEA (2016).

Superintendencia de Bancos e Instituciones Financieras Chile

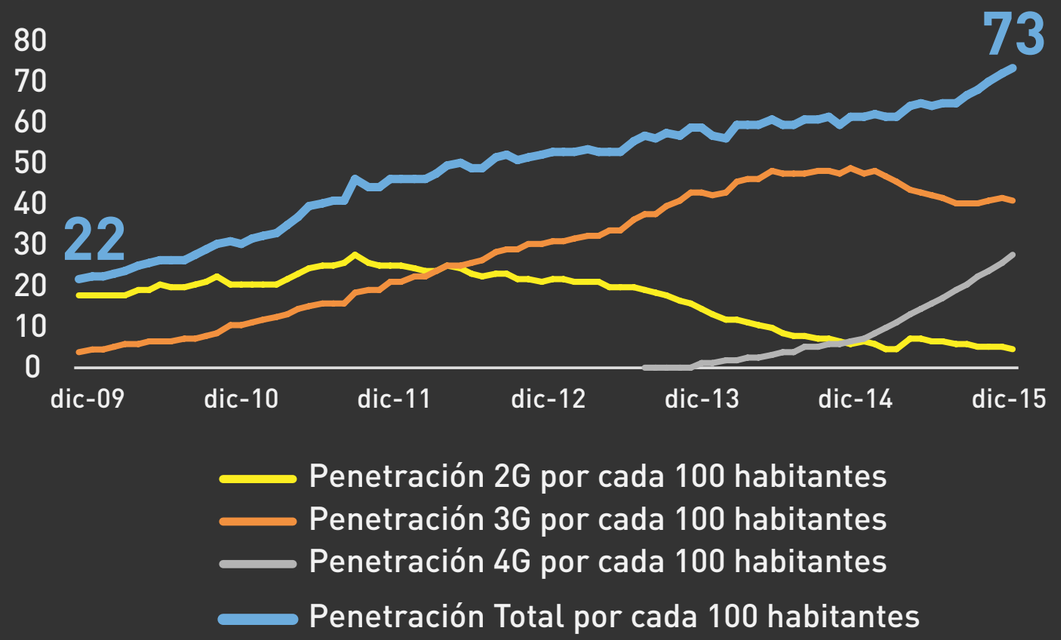
Mientras se observa una creciente penetración de internet en Chile...

La cobertura de la red y su expansión temporal generan importantes perspectivas para el desarrollo de actividades económicas basadas en dichas tecnologías.

Conexiones a internet fija
(conexiones cada 100 habitantes)



Conexiones a internet móvil
(conexiones cada 100 habitantes)



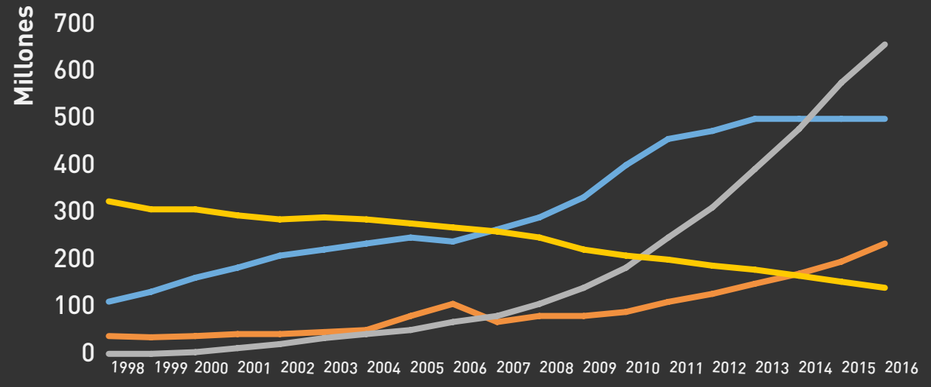
Nota: datos actualizados a septiembre de 2016
Fuente: SUBTEL (2016).

...también aumenta el volumen de operaciones electrónicas...

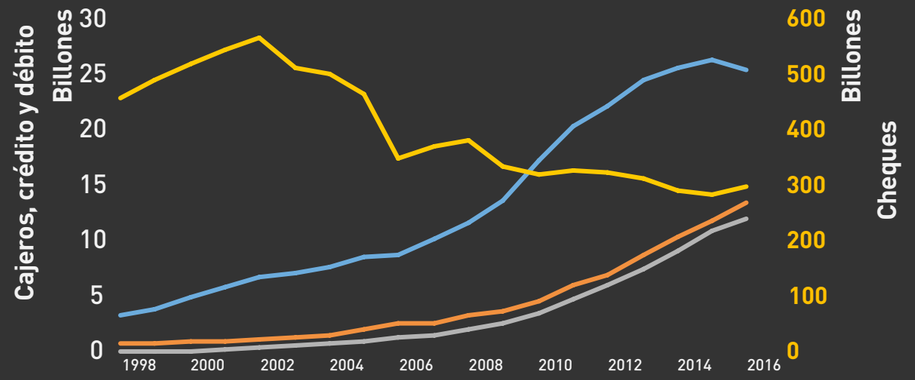
El número de transacciones realizadas a través de cajeros automáticos y tarjetas de pago superan largamente las realizadas por medio de cheques.

En términos de montos, los cheques siguen concentrando una alta proporción de los pagos distintos de efectivo (92%, cifra que en todo caso es 7,7pp menor a la observada durante el año 1998).

Transacciones ATMs, tarjetas de pago y cheques
(número, millones de transacciones por año)



Transacciones: ATMs, tarjetas de pago y cheques
(monto, billones de pesos por año)

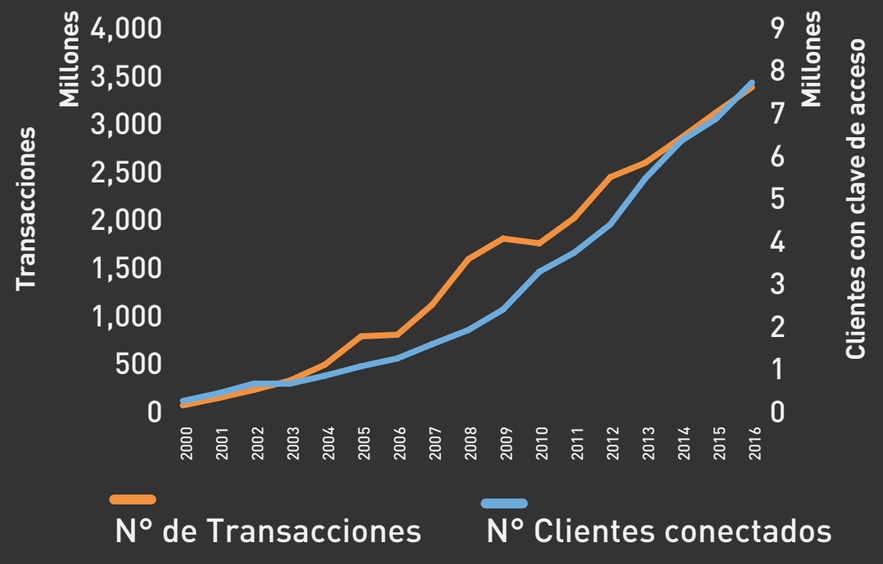


Cajeros Crédito Débito Cheques

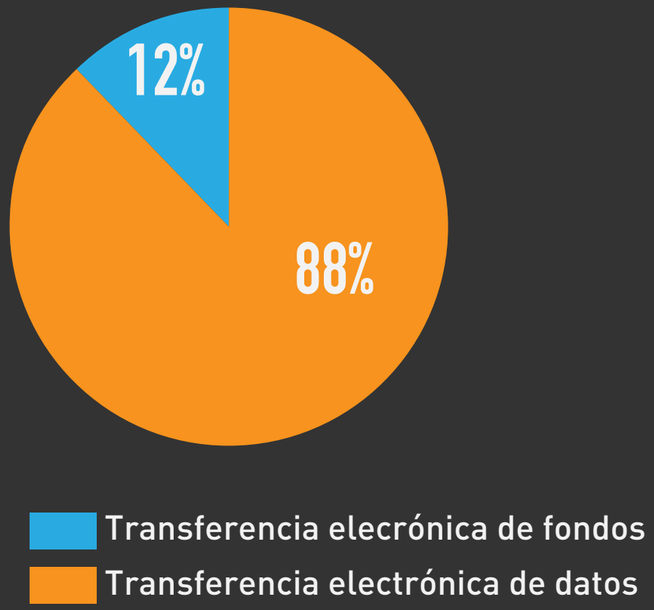
Fuente: **SBIF**

...y de las operaciones bancarias en línea

Clientes y operaciones bancarias realizadas en internet
(número de clientes con clave de acceso y número de transacciones anuales)



Tipos de operaciones bancarias realizadas en internet
(número de transacciones como % del total, 2016)



Fuente: **SBIF**

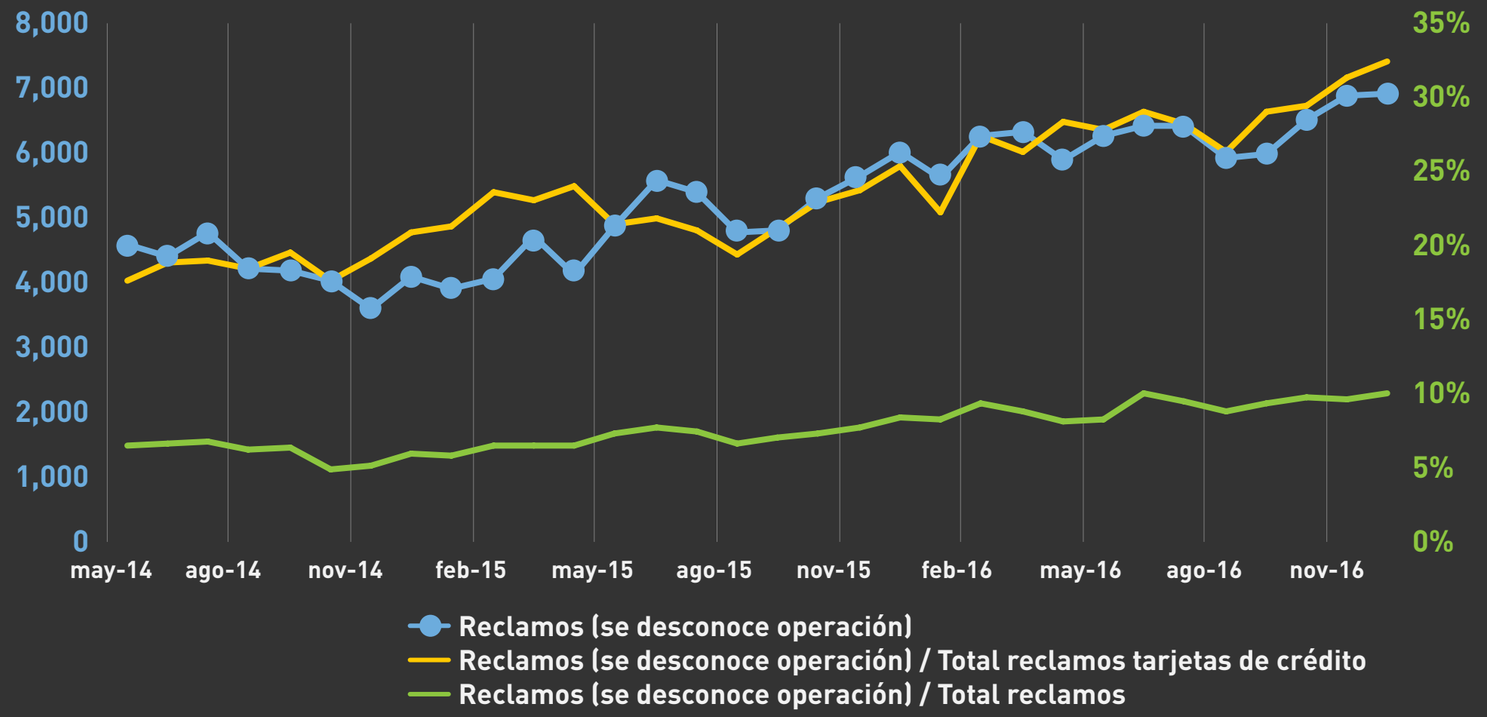
También se observa un aumento en el número de reclamos asociados a tarjetas de crédito...

Los reclamos asociados a situaciones en que el cliente desconoce la realización de operaciones con tarjetas de crédito pasaron de 4.200 mensuales en el año 2014 a 6.200 mensuales en el año 2016.

Una fracción de estas podría estar asociada a ciberdelitos. No existe información oficial respecto a la materia.

Reclamos: cliente desconoce operación

(número y % del total)

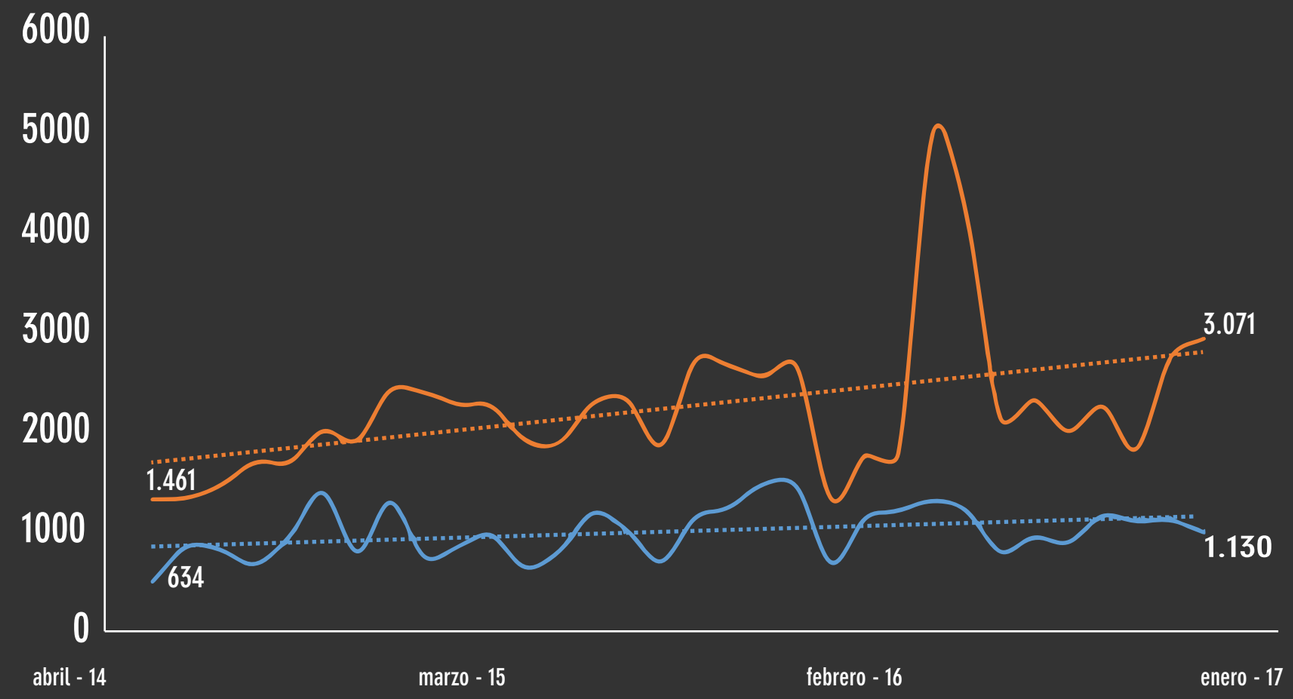


Fuente: **SBIF**

Se observa un aumento en el número de reclamos asociados al “desconocimiento de las operaciones”

· En el caso de las operaciones realizadas a partir de cuentas vistas, los reclamos asociados a situaciones en que el cliente desconoce la operación en canales electrónicos, presenciales o no, aumentaron en un 210% entre el año 2014 y el 2016.

· En el caso de las cuentas corrientes y para el mismo tipo de operaciones, el aumento fue de un 178% en el mismo período.



Fuente: Prensa, medios identificados.

Fuente: **SBIF**

...con un costo reputacional relevante para los bancos, dada su amplia cobertura de prensa

Medio	Fecha	Incidentes
KASPERSKY lab	03/01/2017	Bancos y las organizaciones de pago tienen dificultad para determinar si una transacción es fraudulenta o genuina (Encuesta Kaspersky Lab y B2B International). 38% Admite tener dificultad para manejar el fraude financiero en línea 50% Cree que el fraude financiero en línea está aumentando. 46% Solo ha implementado solución parcial contra el fraude o no han implementado ninguna.

Medio	Fecha	Incidente
El Tipógrafo	07/02/2016	Banda de clonadores es desbaratada e incautan cerca de $21 millones
T13	03/03/2016	Clonación de tarjetas: Desbaratan sofisticada banda y obtienen prisión preventiva de nueve personas
AN AHORA NOTICIAS	03/03/2016	Clonación de tarjetas: desbaratan sofisticada banda y decretan prisión preventiva para nueve personas
EL CENTRO	03/04/2016	Masiva clonación de tarjetas bancarias en solo 24 horas en Talca
emol. Nacional	21/07/2016	Aumentan denuncias y reclamos por clonación de tarjetas en primera parte del año
publimetro	02/09/2016	Más de 200 afectados por clonación masiva de tarjetas en Providencia
emol. Nacional	22/09/2016	Estafas: Bancos deben responder ante clonaciones y giros no autorizados aunque no se tenga seguro
cooperativa.cl	30/09/2016	Carabineros desbarató banda dedicada a la clonación de tarjetas en Puente Alto
Diario Constitucional.cl	04/09/2016	En fallo unánime. Corte de Santiago condenó a banco a pagar multa por clonación de tarjeta.
biobiochile.cl	07/10/2016	Detienen a banda que usaba nuevo e imperceptible método para clonar tarjetas
RADIO VISION	24/10/2016	PDI desarticula banda criminal dedicada a la clonación de tarjetas de crédito y débito en céntrica sucursal bancaria de Temuco
El Observatodo	05/12/2016	Varios habitantes de La Serena afectados por clonación de tarjetas el fin de semana Los cajeros intervenidos se ubican en Cuatro Esquinas y en el centro de la capital de la Región de Coquimbo
elSerenense	06/12/2016	La PDI, recibió 21 denuncias por uso malicioso de tarjetas de crédito en cajeros automáticos en la ciudad de La Serena.

Las denuncias por uso fraudulento de tarjetas de crédito y débito también han aumentado

El uso fraudulento de tarjetas de debito y crédito es hoy uno de los delitos con mayor crecimiento.

Denuncias por uso fraudulento de tarjetas de crédito y débito

	dic-13	dic-14	dic-15	jun-16
Denuncias	15.313	17.683	34.359	28.209
Variación 12 meses		16%	94%	123%

Fuente: **Ministerio Público**

El país está realizando importantes esfuerzos para mejorar sus capacidades en materia de ciberseguridad

Hito	Fecha	Alcance
Promulgación Decreto 533 Comité Interministerial sobre Ciberseguridad)	Julio de 2015	• Integrantes: subsecretarías de Interior, Defensa, Relaciones Exteriores, Justicia; Secretaria General de la Presidencia, Telecomunicaciones, Economía, Hacienda, en calidad de invitado, y la Agencia Nacional de Inteligencia. • Principal objetivo: "crear una Política Nacional de Ciberseguridad, que resguarde la imagen, dignidad y honor de las personas; combata la propagación de material que transgreda su intimidad; y que sea implacable al perseguir delitos relacionados con la pornografía infantil".
Consulta Ciudadana sobre Política Nacional de Ciberseguridad	Febrero de 2016	• En cumplimiento de la misión encargada mediante Decreto Supremo Nº533 de 27 de abril de 2015, el Comité Interministerial abrió una consulta ciudadana sobre la Política Nacional sobre Ciberseguridad. Los resultados de la consulta fueron publicados el 15 de abril de 2016.
Finaliza tramitación (Congreso) para ratificación del Convenio de Budapest	Noviembre de 2016	• Iniciativa presidencial que sometió a aprobación el"Convenio sobre la Ciberdelincuencia", suscrito en Budapest, Hungría, el 23 de noviembre de 2001. Acuerdo (ratificado por alrededor de 50 países) que tiene como principal objetivo el desarrollo de una política criminal común frente al ciberdelito (homologación de la legislación y establecimiento de un sistema de cooperación internacional).

La SBIF también ha incorporado esta materia en su agenda de trabajo

Hito	Fecha	Alcance
Seminario sobre ciberseguridad (SBIF – Ministerio del Interior)	Mayo de 2016	Medidas que se pueden aplicar para enfrentar la irrupción de cibercrimen en los sistemas de pagos.
Carta Circular N° 1-2016 Bancos (SBIF)	Junio de 2016	SBIF emite norma sobre seguridad de la Información y Ciberseguridad. Enfatiza la necesidad de tomar medidas de control.
Mesa de trabajo público –privada de ciberseguridad (SBIF-ABIF-Ministerio del Interior)	Septiembre de 2016	Enfrentar delitos de clonación de tarjetas y la actualización de medidas de seguridad de cajeros automáticos.
Campaña preventiva (SBIF-ABIF-Ministerio del Interior)	Septiembre de 2016	SBIF, ABIF, Carabineros de Chile y la PDI, difundieron por redes sociales y de manera presencial, un conjunto de medidas preventivas para evitar la clonación de tarjetas en el país.
Seminario sobre ciberseguridad (SBIF y Embajada Británica)	Septiembre de 2016	La actividad (seminario Mind the Gap) se enfocó en los desafíos que representa la seguridad tecnológica e informática en la industria financiera.
Pasantía Ciberseguridad Reino Unido	Enero de 2017	Reuniones con reguladores y empresas de ciberseguridad: Bank of England, Financial Conduct Authority, CREST, HM Treasury, Control Risk, Level 39, entre otros.

Superintendencia de Bancos e Instituciones Financieras Chile

Comentarios Finales

- Equilibrio entre los beneficios derivados del uso de la tecnología y el control de los riesgos asociados.
- Desde una perspectiva macro:
  - La ciberseguridad es una tarea que involucra a múltiples sectores (privado, público, comunidad internacional, reguladores, y usuarios, entre otros) y múltiples funciones (sensibilización, regulación, autorregulación, tecnología, gestión de riesgos, educación financiera, etc.).
  - Experiencia internacional: Más que soluciones tecnológicas específicas, es relevante la coordinación, cooperación y el intercambio de información entre los actores.

Comentarios finales

- Desde una perspectiva micro:

  · Participación activa de la alta administración de las entidades en la gestión de los riesgos asociados al ciberespacio.

  · Generación de estrategias de gestión robusta:

    · Identificación de los riesgos.
    · Mecanismos de detección y control.
    · Generación de planes de continuidad operacional.
    · Evaluación continua de la efectividad, entre otros.

  · Se propone la generación de una base de datos de incidentes compartida en la industria, que permita el aprendizaje y la prevención.

  · La educación de los usuarios, la protección de las claves y el resguardo de su información, el autocuidado.

Próximos pasos para la SBIF

· La generación de un programa de corto y largo plazo asociado a materias de ciberseguridad.

· La promulgación de normas que fortalezcan el sistema en materias de ciberseguridad.

· Generación de estrategias y planes de trabajo (IFIS).
· Revisión de los roles y responsabilidades de los agentes involucrados.
· Educación para usuarios y la responsabilidad de las instituciones en la entrega de información necesaria para el uso de sus productos.

· La generación de foros, seminarios, ferias, entre otros, que permitan la sensibilización del entorno, de la industria, de los usuarios, del fiscalizador.

Superintendencia de Bancos e Instituciones Financieras Chile

Próximos pasos para la SBIF

La forma en que las instituciones atienden a los usuarios afectados y responden frente a eventos de ciberfraude es clave para mitigar su impacto. En el negocio financiero no existe un activo más relevante que la confianza y la reputación.

Superintendencia de Bancos e Instituciones Financieras Chile

Ciberseguridad en la Industria Financiera

Eric Parrado H. (@eric_parrado)
Superintendente de Bancos e Instituciones Financieras

15 de marzo de 2017
RBECA Liquidnexus

Referencias

· BID-OEA (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?. Informe Ciberseguridad 2016, Observatorio de ciberseguridad.

· CSIS - McAfee (2014). Net Losses : Estimating the Global Cost of Cybercrime. P.23, 2014 Center for Strategic and International Studies and McAfee. Obtenido de http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

· Prandini, Patricia y Marcia L. Maggiore (2011). Panorama del ciberdelito en Latinoamérica. Documento de trabajo. Montevideo: Registro de Direcciones de Internet para Latinoamérica, 2011.

· Ponemon Institute (2016). Cost of Cyber Crime Study. Research Report Publication Date: October 2016. Obtenido de: http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s

SUBTEL (2016). Estadísticas de conexiones a internet. Serie de Estadísticas Sectoriales, Subsecretaria de Telecomunicaciones de Chile. Consultado en: http://www.subtel.gob.cl/estudios-y-estadisticas/internet/

UIT (2015). Índice mundial de ciberseguridad y perfiles de ciberbienestar. Unión Internacional de Telecomunicaciones, abril de 2015. Obtenido de: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf