# Ciberseguridad y ciberinteligencia para la protección en el sector financiero

# WELCOME

# Estado del arte


Sector financiero y Ciberseguridad

# Seguridad percibida vs. Seguridad real

# Seguridad percibida vs. Seguridad real


**Gráfica Nº. 8. Situaciones vividas en los últimos 12 meses que atentaron contra su seguridad y/o delito-Lugar en donde ocurrió el delito o hecho violento / Respuestas múltiples.**

Base: Víctimas de delito (198) / Datos en %

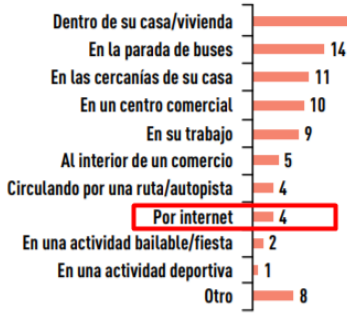

**"El 50% de los casos ocurrió en la vivienda o en las cercanías a ésta".**

El 33% de los hechos reportados sucedió en la casa y 17% en las cercanías a la misma. Preocupa esta situación porque el hogar se convierte en un sitio vulnerable, generando una doble victimización, debido a que involucra al sujeto residente, familiares y a la misma residencia.

**Gráfica Nº. 12. HURTO**

(Base: Víctimas de Hurto (103) / Datos en %

**Lugar en donde ocurrió**




***El hurto ocurre en un 45% dentro de su casa/ vivienda o en las cercanías a ésta, 14% en la parada de buses,*** *10% en un centro comercial y 9% en su trabajo. En menor proporción, en el interior de un comercio (5%), 4% circulando por una ruta/ autopista y por internet, 2% en una actividad bailable o fiesta y 1% en una actividad deportiva.*

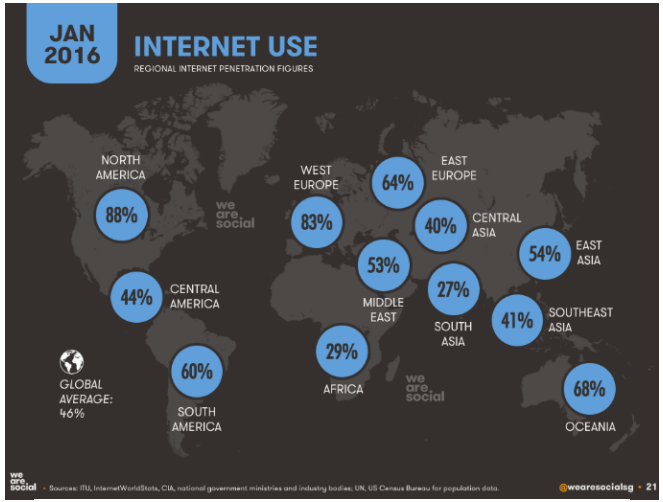
# Uso de Internet en América Latina

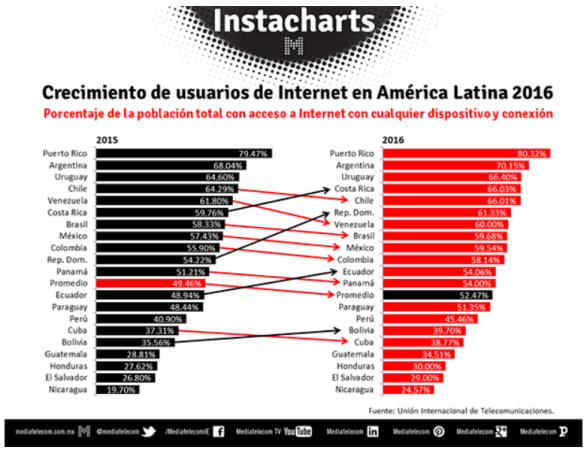
## Uso de canales (al menos de forma semanal)

| | Total |
|---|---|
| Sucursal u oficina | 24% |
| *Call center* | 12% |
| Cajero automático | 58% |
| Internet/*online* | 57% |
| Celular | 30% |
| Promedio de uso de canal remoto * | 48% |

* Cajeros, celulares, internet/online

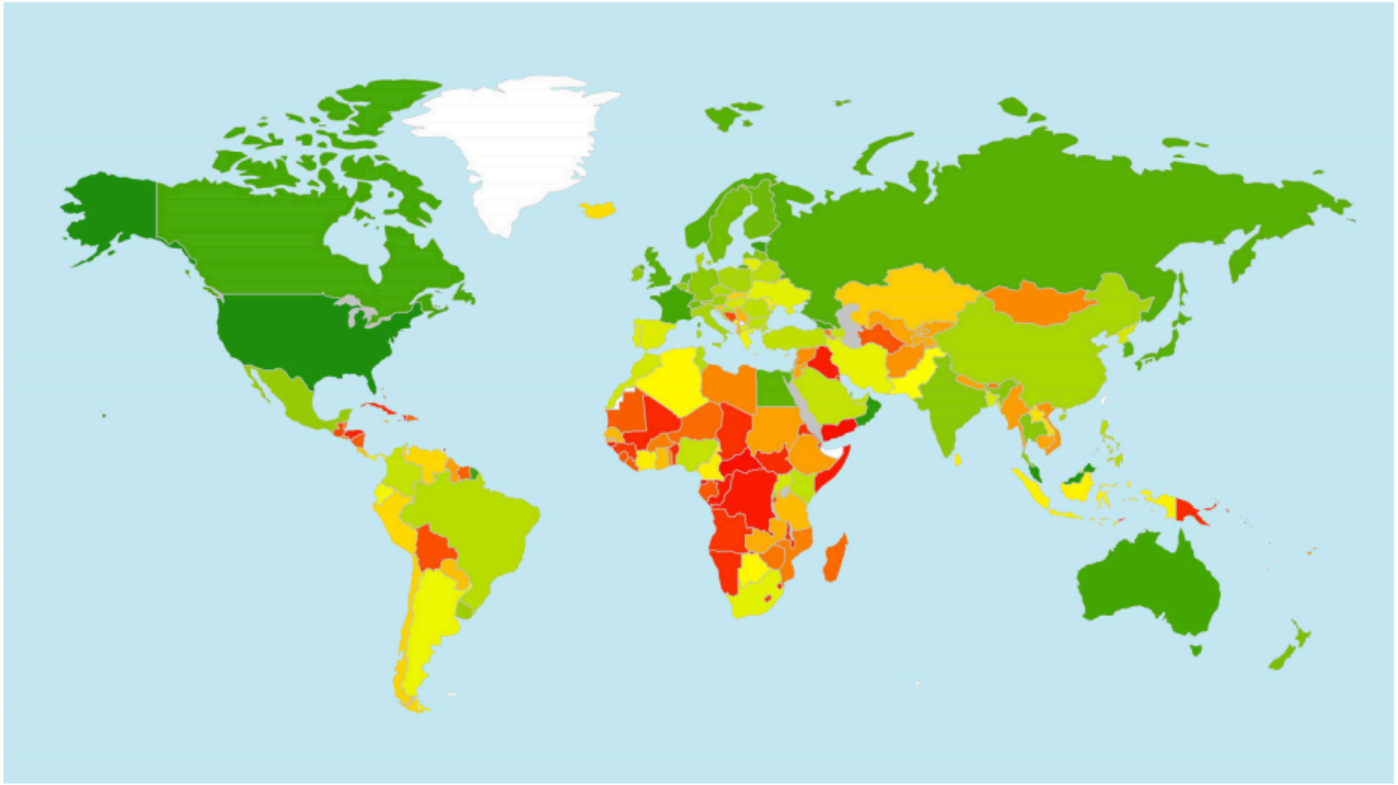
Fuente: Ganar a través de la experiencia del cliente: encuesta EY a clientes de la banca minorista 2014 - EY



# Nivel de compromiso de países en materia de ciberseguridad

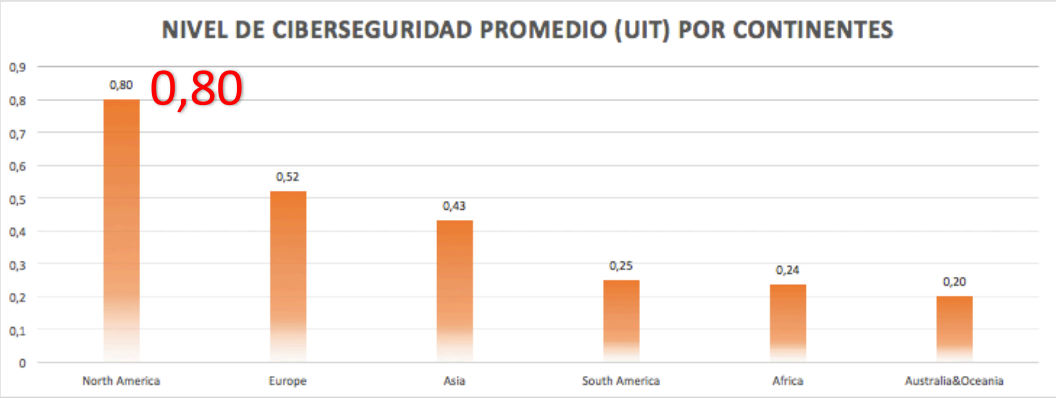
Nivel de compromiso: de verde oscuro (muy alto) a rojo (muy bajo)

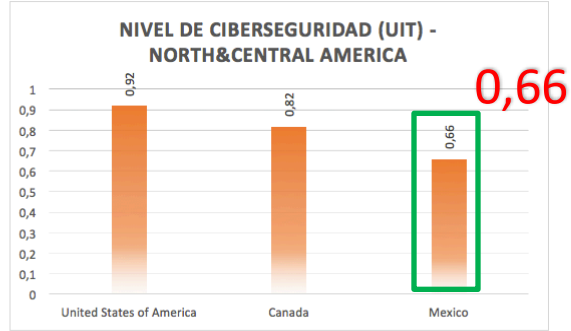


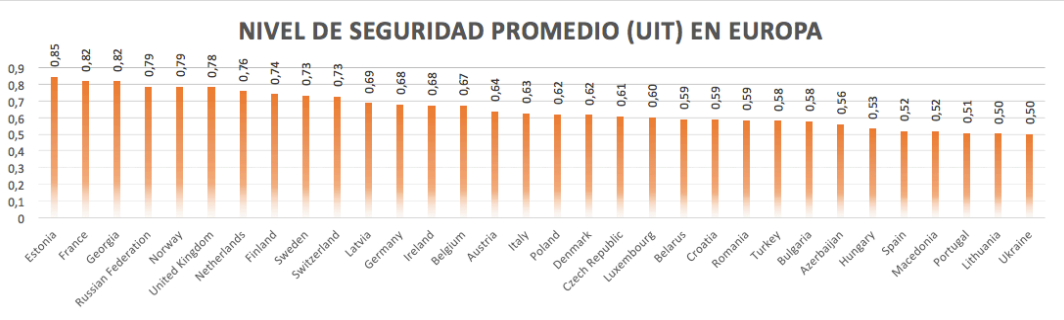
Fuente: Global Cybersecurity Index (GCI) ITU –2017

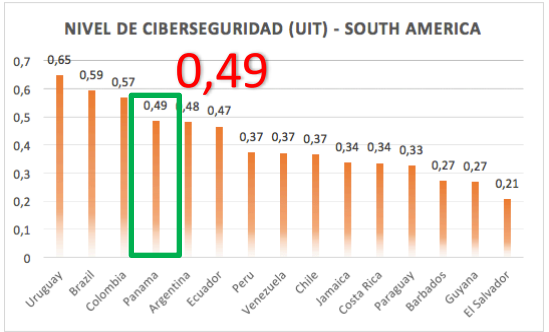
# Nivel de compromiso de países en materia de ciberseguridad

Score: Nivel Máximo: 1; Nivel mínimo: 0




Fuente: Global Cybersecurity Index (GCI) ITU –2017

# Encuesta sobre riesgos de seguridad para instituciones financieras


**Hoy:**

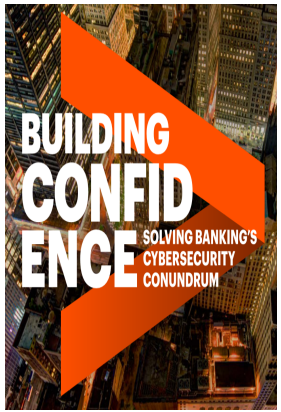
- **80%** clientes operan en Internet
- **33%** de los bancos ha registrado incidentes de seguridad online

**Mañana:**

- **25%** de los bancos tendrá dificultades de verificación de identidad
- **60%** prevén pérdidas contables por fraude en los próximos 3 años

Fuente: Karpesky Lab – Enero 2017

# Informe de ciberseguridad para el sector financiero




Fuente: Accenture– 2016

- **La percepción:**
  - Existe conciencia de las amenazas
  - Ambas partes del "conflicto" progresan en la evolución tecnológica
  - **78%** de los ejecutivos entrevistados muestran confianza en sus sistemas de protección


- **La realidad …**
  - **40%** de los ataques provienen de *insiders*
  - **85%** de los bancos sufrieron amenazas serias en los últimos 12 meses
  - **36%** fueron exitosos
  - **59%** fueron detectados después de…

…**varios meses**!!!


"Para el año 2019, los costos globales del cibercrimen alcanzarán los 2 billones de dólares anuales", señala la OCDE, **dos veces el PIB de México todos los años**!

# ¡No se puede proteger lo que no se reconoce vulnerable !!

## ¿Somos vulnerables?

# Transformación digital en el sector financiero

Un modelo nuevo con nuevos componentes

# Transformación digital en el sector financiero

## ¿Sabías que?

Kotak Mahindra, el cuarto mayor banco del sector privado de la India, ha puesto en marcha "Jifi": una cuenta de banco que integra las plataformas de medios sociales. Los clientes pueden abrir una cuenta Jifi inscribiéndose a través de Facebook o correo electrónico, recibir actualizaciones de cuentas bancarias a través de Twitter y ganar puntos de recompensa para las transacciones en línea y añadir contactos a su red Jifi.

Fuente: Leading through innovation: the future of bank in emerging markets 2016 - EY

## ¿Sabías que?

En Polonia, los clientes pueden usar un aplicativo desde su smartphone para solicitar un ATM móvil adaptado en un BMW eléctrico (cajero móvil) que va al punto que lo pidas.

Fuente: Leading through innovation: the future of bank in emerging markets 2016 - EY

## ¿Sabías que?

47%

de las ocupaciones en las economías avanzadas tiene un 'alto riesgo' de ser automatizadas en los próximos 20 años.

Fuente: Transforming talent, the banker of the future: global banking outlook 2016 - EY

## ¿Sabías que?

En el 2020, habrá 2,000 millones de usuarios de smartphones biométricos, 10 veces más de los que hubieron en el año 2010.

Elaboración: Global Markets EY

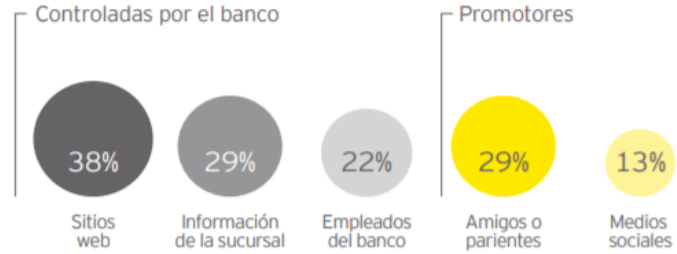
US$8,000 millones representará el mercado de tecnología biométrica para el sector financiero en el 2020.

Elaboración: Global Markets EY


Elaboración: Global Markets EY

# Transformación digital en el sector financiero

**Principales fuentes de información utilizadas al momento de buscar un proveedor de servicios financieros**




Fuente: Ganar a través de la experiencia del cliente: encuesta EY a clientes de la banca minorista 2014 - EY

**Segmentos de clientes y penetración por producto**

| | Grande | Élites | Vanguardistas | Prácticos | Conservadores | Tradicionales | Autosuficientes | Insatisfechos e incrédulos | Total |
|---|---|---|---|---|---|---|---|---|---|
| **% Población** | 6% | 11% | 12% | 10% | 22% | 15% | 14% | 10% | 100% |
| **Edad (en años)** | | | | | | | | | |
| 18 - 34 | 43% | 26% | 44% | 27% | 41% | 39% | 32% | 33% | 36% |
| 35 - 49 | 37% | 31% | 29% | 35% | 24% | 25% | 26% | 27% | 28% |
| 50 o mayor | 20% | 43% | 27% | 38% | 35% | 36% | 42% | 40% | 36% |
| **Tipo de producto** | | | | | | | | | |
| Banca electrónica | 92% | 95% | 90% | 97% | 47% | 14% | 97% | 56% | 69% |
| Pagos por celular | 87% | 39% | 61% | 13% | 13% | 14% | 11% | 9% | 26% |

Fuente: Ganar a través de la experiencia del cliente: encuesta EY a clientes de la banca minorista 2014 - EY

# Transformación digital en el sector financiero

- Ataques internos
- Ataques hacktivistas/ ideológicos
- Ataques dirigidos
- Crime-as-a-service

# Conciencia del Problema:
# Evaluación de las estrategias de ciberseguridad; Preguntas críticas

¿Tenemos **estrategia de Ciberseguridad**?

¿Nuestra **estrategia** corporativa está **alineada** con la seguridad requerida?

¿Estamos seguros de conocer los **activos críticos** de nuestro negocio y su localización?

¿Conocemos a **nuestro atacante**, qué herramientas usa y cuales son sus técnicas?

¿Están consejeros, directivos y trabajadores suficientemente **educados** para entender los riesgos?

¿Cuál es nuestro ratio de **riesgo outsiders / insiders**?

¿Cómo afectan los **cambios regulatorios** en las estrategias de ciberseguridad?

¿Disponemos de suficientes **recursos** (económicos y humanos)?

# Prevención + Orientación a Detección Temprana, junto con una rápida y efectiva Disrupción del Ataque.

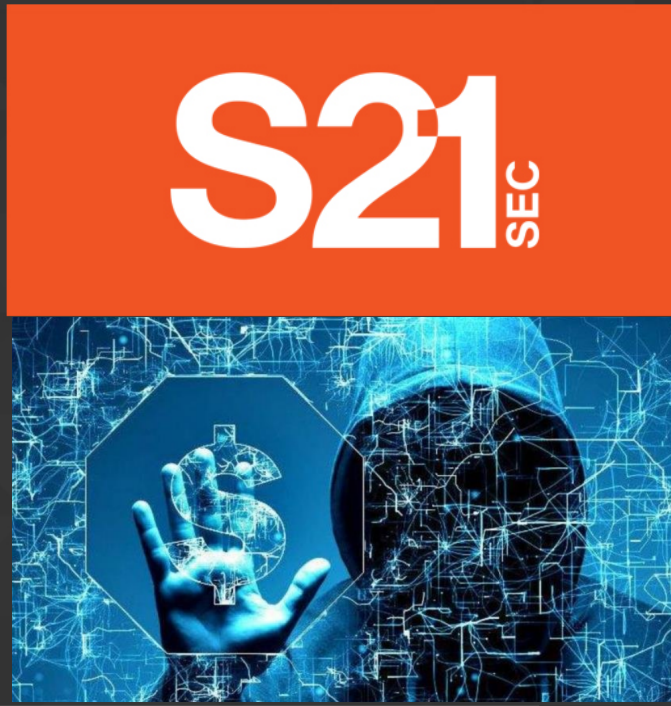
**“Las organizaciones gastan millones de dólares en *firewalls* y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores”.**

***Kevin Mitnick (Hacker)***

# Ejemplos

ATAQUES a MEXICO y CHILE

MEXICO: Una operación digna de una película de Hollywood



# Ataque SPEI MEXICO

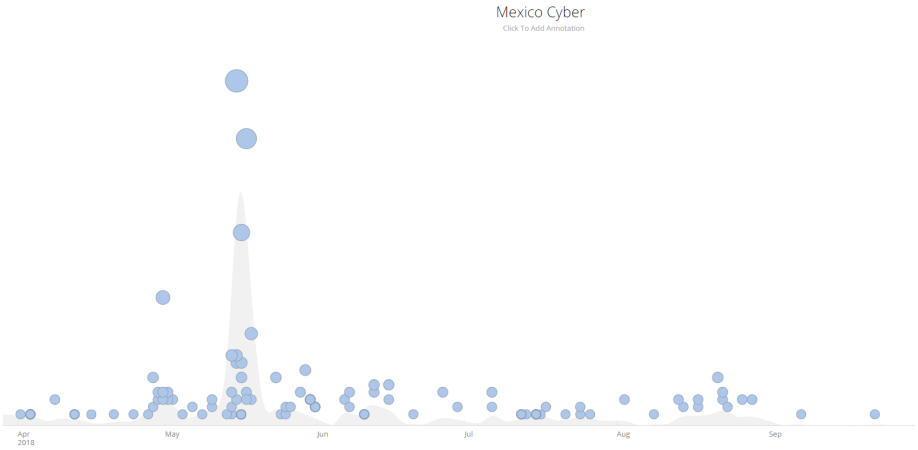
"Ataque de sofisticación tecnológica, humana y logística"

"No hubo afectación a los clientes usuarios"

"15 Mill USD en retiros de 10,000 USD de media en cientos de cuentas"

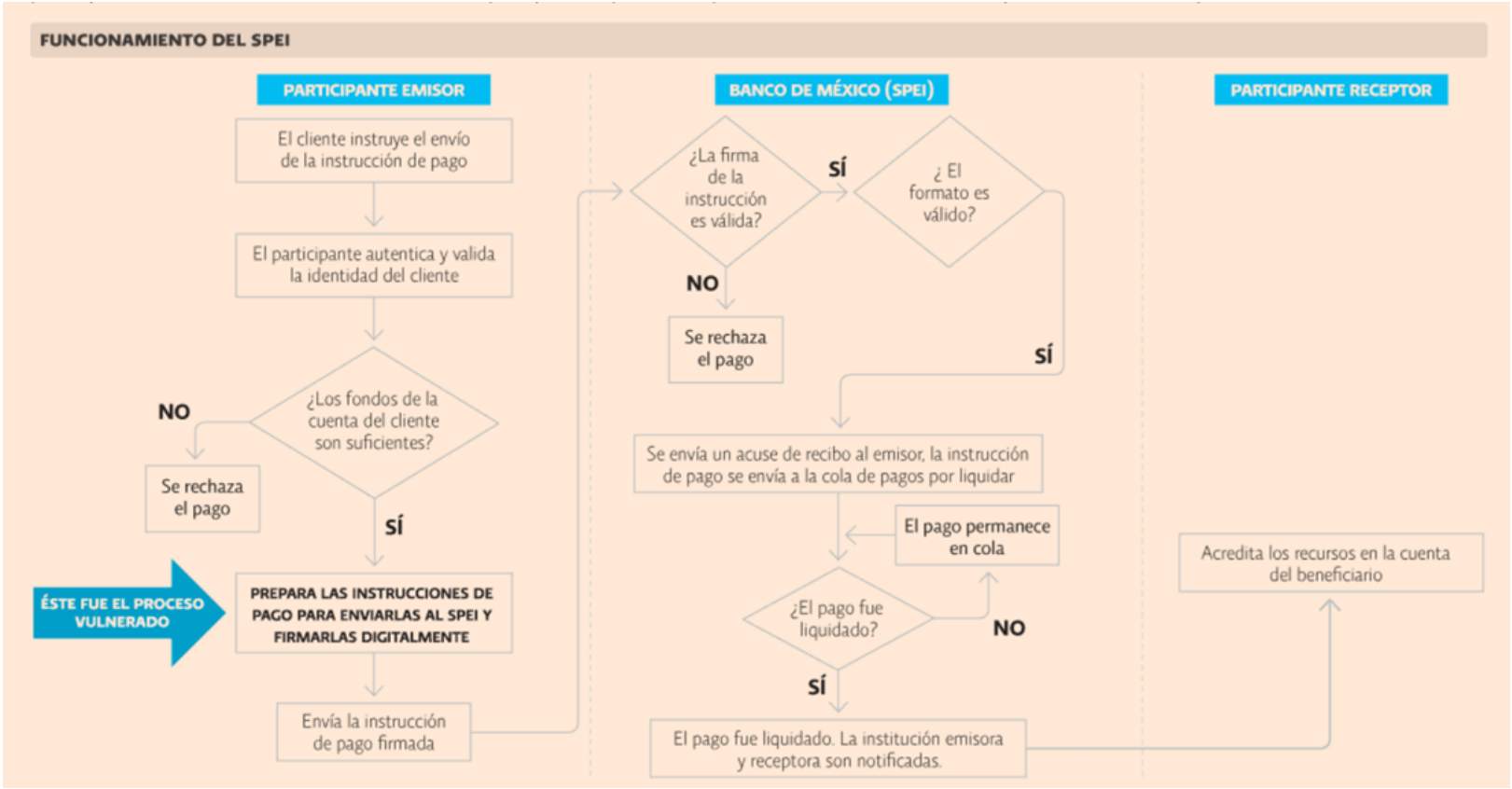
"Tecnológicamente fue sobre el aplicativo (API) de acceso al SPEI"

"Los retiros fueron en cuentas de más de 5 bancos mexicanos"




*A. Diaz de León, Gobernador Banxico*

# Ataque SPEI MEXICO



# Ataque SPEI MEXICO

1. Un grupo de *hackers* ataca a los proveedores de instituciones financieras que se conectan al SPEI.

2. Los *hackers* sustraen recursos de las cuentas concentradoras de los bancos.


3. Los recursos se reparten en cuentas bancarias individuales de delincuentes y de algunos comerciantes.

4. Los involucrados recibieron pagos por permitir usar su cuenta y hacer retiros de los recursos sustraídos.

5. Los cómplices acuden a hacer los retiros en diferentes sucursales bancarias.

6. Hecho el retiro, los involucrados entregan el dinero a los ciberdelincuentes en efectivo.

# Ataque al Banco de Mexico – Ciberataque sofisticado


BANCO DE MÉXICO

1. Primer conocimiento del evento a través de redes sociales.
2. Alto tiempo de preparación e investigación de los bancos mexicanos.
3. Los Hackers realizan transacciones ficticias contra cuentas de los bancos y casas de bolsa a cuentas destino previamente orquestadas.
4. Ataque local con alta logística en la recuperación del efectivo.
5. Tardan **100** días en entender lo que ha sucedido

# Ataque al Banco de Chile

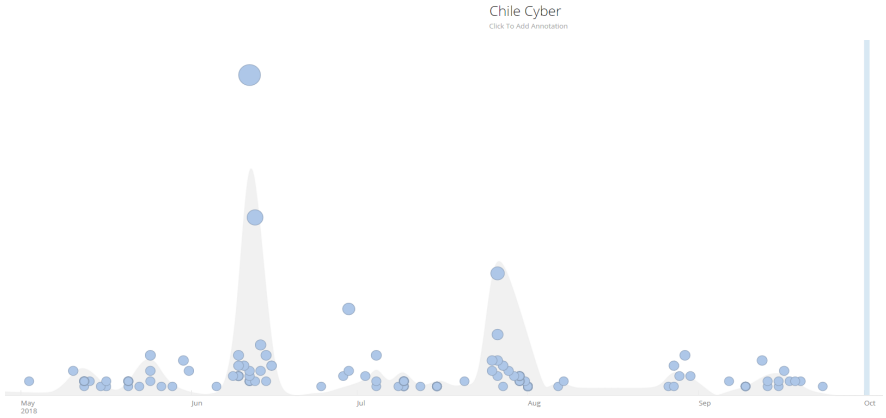
"Encontramos algunas transacciones extrañas en el sistema SWIFT."

"Ningún cliente se vio afectado, pero los atacantes robaron US$10 millones al banco."

"Éste era un evento destinado a **dañar al banco**".

"Una banda de Europa del Este o Asia sería la culpable del ciberataque."

"Éste es un nuevo método que desde Chile lo veíamos un poco lejos, pero ahora viene bajando a Latinoamérica".




*Eduardo Ebensperger. Gerente general de Banco de Chile*

# Ataque al Banco de Chile – Ciberataque sofisticado


1. BdC reacciona bloqueando las operaciones de 9,000 sucursales (Bloqueo de la Banca Online).
2. BdC consigue detener todas las transacciones menos 4 que provocan un fraude de 10Mill USD.
3. Tardan 4 días ininterrumpidos en parar el hackeo.
6. Alta innovación informática del ciberataque.
7. Exhaustivo análisis de los procesos y operaciones del Banco de Chile.
8. Ciberataque internacional (Europa del Este/Asia).


ESTRATEGIA

# SOME QUICK WINS

- *Analicemos las **fuentes abiertas** (ciberinteligencia) y comparémosnos (**ratings**)*
- *Conozcamos a los actores y sus motivaciones.*
- *Conozcamos nuestro sector y las tendencias en ciberseguridad.*
- *Preparemos planes de protección y mitigación ante Ransomware, Malware, y DDoS. **Actualicemos los Parches!!***
- *Observemos a nuestros **empleados***
- *Auditemos a nuestros **proveedores***
- *Usemos **doble factor de autenticación** en todas las apps Web*

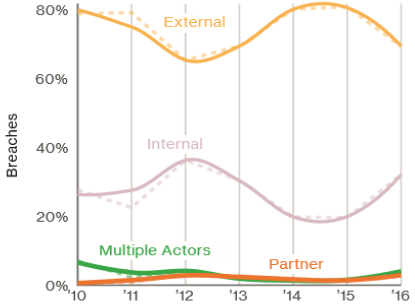
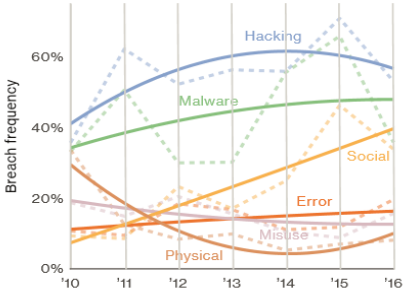
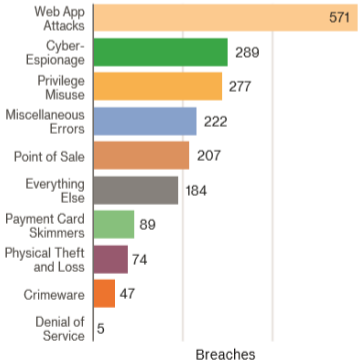
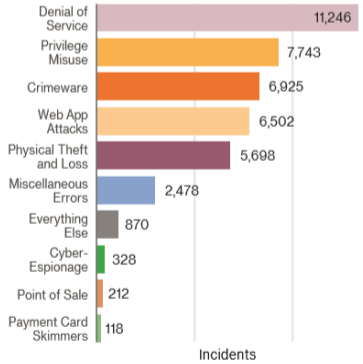



Figure 2: Threat actor categories over time

banking Trojan botnets and POS. Organized criminal groups continue to utilize ransomware to extort money from their victims, and since a data disclosure in these incidents is often not confirmed, they are not reflected in Figure 3.



# ¡Gracias!


Laura Requena Espada
Manager Inteligencia
lrequena@s21sec.com