PUBLICACIÓN No. 4 | JULIO 22 DE 2020 | BOGOTÁ - COLOMBIA

CÁPSULAS SOBRE Ciberseguridad

AL DÍA CON FELABAN

Radiografía de un "Data Breach" o Fuga de Información

FIC

FRAUD INFORMATION CONTROL
by FELABAN

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

55 AÑOS
1965 - 2020

Radiografía de un "Data Breach"o Fuga de Información

Un "Data Breach", fuga de información o ingreso no autorizado a datos con accesos restringidos, es uno de los temores empresariales de estos tiempos. Las empresas, los gobiernos y las personas cada vez sienten más, que su información puede no ser segura en sus diferentes dispositivos y que las empresas no pueden garantizar al 100% la integridad de esta. No en vano Nancy Donahue, Gerente del foro de riesgos del sistema de pagos minorista en el Banco de la Reserva Federal de Atlanta, menciona que **"las amenazas pueden venir de muchas formas, como sabemos, desde el riesgo interno a los actores externos, o incluso a los socios o proveedores de la compañía, por lo que es importante mirar hacia adentro, así como hacia afuera"**[1].

Para las empresas que resguardan la información de sus clientes, es un reto que implica una intensa planificación. Las fugas, pueden ocurrir por una falta de protocolos de seguridad tanto en el proceso de encriptación u otros métodos de protección de datos, como en administración de perfiles de acceso a datos que se encuentran en computadores, discos duros, archivos físicos, servidores u otros dispositivos electrónicos.

Bien sea de manera intencional o no intencional, la prevención ante eventos de fuga de información es muy importante, ya que estas no solo pueden acarrear costos y daños a la empresa que resguarda los datos, sino también consecuencias considerables de los ciudadanos que confían dicha información a las diferentes organizaciones.

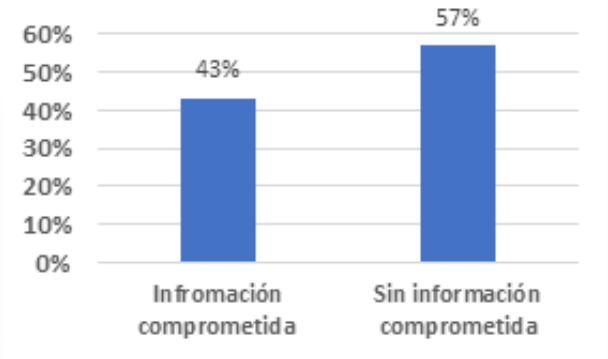
Las empresas hoy enfrentan un compromiso, ético y legal ante las personas que depositan sus datos en el marco de la buena fe. Por esto, es vital que todas cuenten con mecanismos de cumplimento en protección de datos, planes de evaluaciones de riesgo, instrumentos de vigilancia internos, protocolos de información sobre posibles incidentes, y planes de auditoria permanente y mejora continua en el resguardo de dichos datos.

1. https://www.frbatlanta.org/podcasts/transcripts/economy-matters/200130-data-breach-prevention

Cifras actuales para la Industria Financiera y otras Industrias

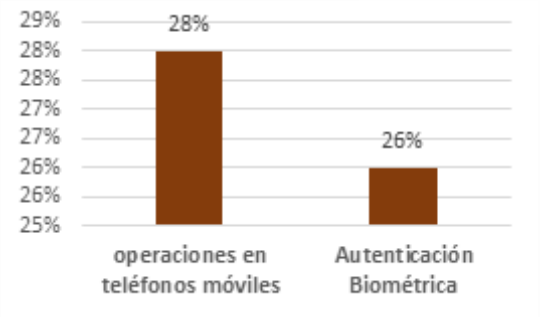
De acuerdo con el reporte "Consumer Loss Barometer The economics of Trust" de la firma KPMG publicado en 2019, indicó lo siguiente para la región de las Américas:

% de Información Financiera comprometida de total de encuestados



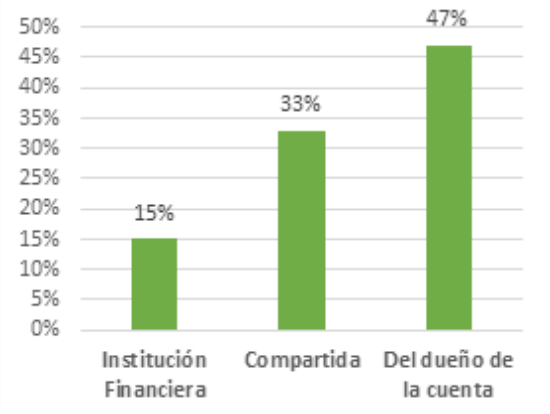
Fuente: Fuente: KPMG, 2019, Consumer Loss Barometer The economics of Trust. Elaboración propia.

% de encuestados que no se sienten comodos con operaciones digitales



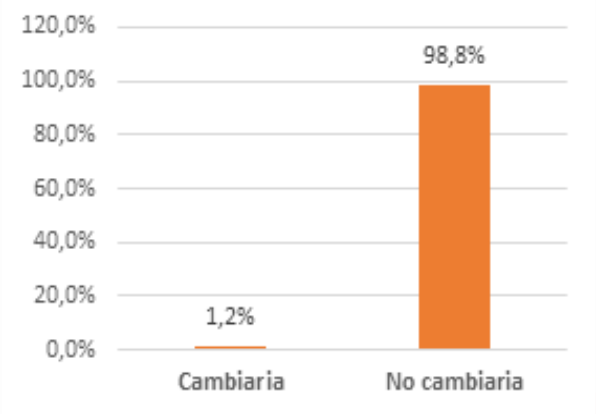
Fuente: Fuente: KPMG, 2019, Consumer Loss Barometer The economics of Trust. Elaboración propia.

Responsabilidad de la seguridad de los datos



Fuente: Fuente: KPMG, 2019, Consumer Loss Barometer The economics of Trust. Elaboración propia.

% de clientes que cambiarian proveedor financiero tras evento de fuga de infomación

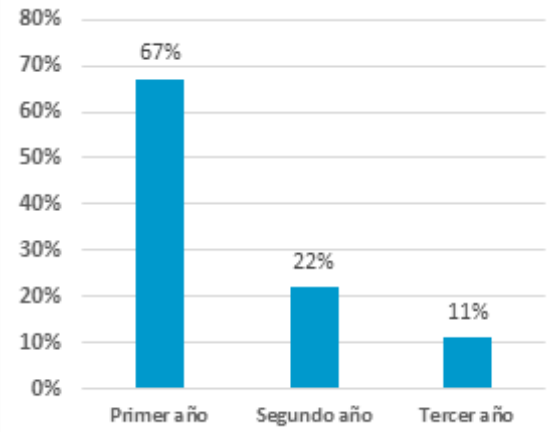


Fuente: Fuente: KPMG, 2019, Consumer Loss Barometer The economics of Trust. Elaboración propia.

Adicionalmente, de acuerdo con un reporte de la firma IBM Security publicado en 2019 "Cost of Data Breach", en el cual se analizaron reportes de 507 empresas en 16 países y 17 industrias, el costo promedio de un evento de fuga de información es de 3.92 millones de USD, con un promedio de datos fugados de 25.575 registros. Estados Unidos, figura como el país más costoso con 8.19 millones de USD en promedio y la industria de la salud, la más costosa con 6.45 millones de USD en promedio.

De igual manera, IBM reportó que de los 3.92 millones de USD en costo promedio de estos incidentes, el 36 % (1.42 millones) representan el costo de perdida de negocio generado por el evento adverso. Las organizaciones en las que se pierden menos del 1% de sus clientes que experimentaron fugas de información, sufren un impacto de costo total promedio de cerca del 2.8 millones de USD.

Tiempo de materialización de fraude tras un evento de fuga de información



Fuente: KPMG, 2019, Consumer Loss Barometer
The economics of trust. Elaboración propia.

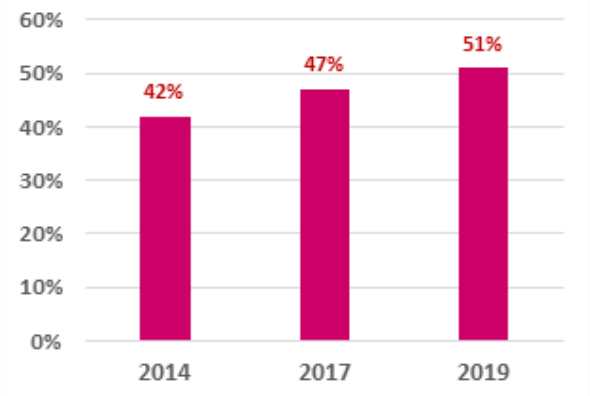
Impacto financiero de un evento adverso y su costo

Fuente: Fuente: KPMG, 2019, Consumer Loss Barometer
The economics of Trust. Elaboración propia. . En este gráfico se tiene en cuenta el ciclo de vida de un incidente de fuga de datos, donde se relacionael tiempo de identificación del mismo y el tiempo necesario para contenerlo.

Esto responde a que el ciclo de vida de una fuga de información se está volviendo más largo. En 2019 se tomaba 206 días en identificar un evento negativo y 73 días en contenerlos, aproximadamente 9.3 meses, mientras que en 2018 el tiempo total era de 8.8 meses.

El 59% de las fugas de información son derivadas fallos en los sistemas (25%) y de error humano (24%). Sin embargo, la causa más importante es la de ataque criminales o afectación por código malicioso el cual representa el 51%, tendido una tasa un impacto de costo por registro de 132 USD (fallos de sistemas), , 133 USD (error humano) y 166 USD (código malicioso).

Crecimiento en ataques maliciosos o criminales con causa de fugas de información (%)



Fuente: KPMG, 2019, Consumer Loss Barometer
The economics of trust. Elaboración propia.

Tener terceros involucrados en el día a día del negocio, puede generar riesgos. Operaciones de migración a la nube, fallas de cumplimiento, sistemas complejos y tecnología operacional son de los competentes que más trae costos adjuntos, dejando resultados en empresas de 500 a 1.000 empleados, costos de 3.533 USD por empleado y 2.65 millones de USD en total y en empresas de más de 25.000 empleados costos totales de 5.11 millones de USD.

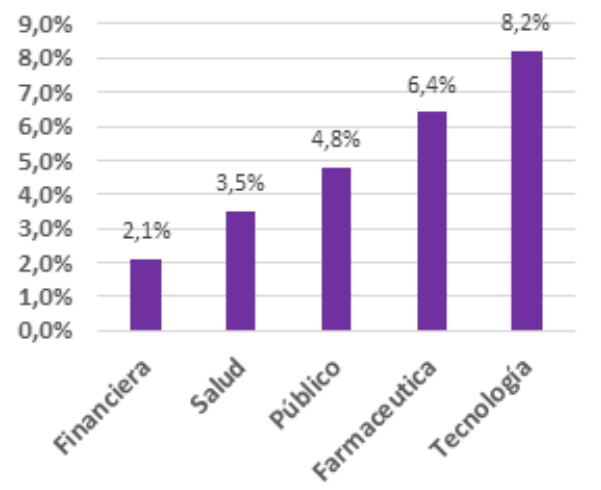
El mundo financiero lejos de ser inmune

En cuanto a la industria financiera, el costo total promedio de un evento adverso tras una fuga de información es de 5.86 millones de USD representando el 2.1% de cambio neto entre 2018 – 2019 del costo total de la industria financiera, ocupando el segundo lugar tras la industria de la salud, la cual tiene una medida de 6.45 millones de USD.

Crecimiento del costo ante un incidente adverso de fuga de datos 2018-2019 (%)

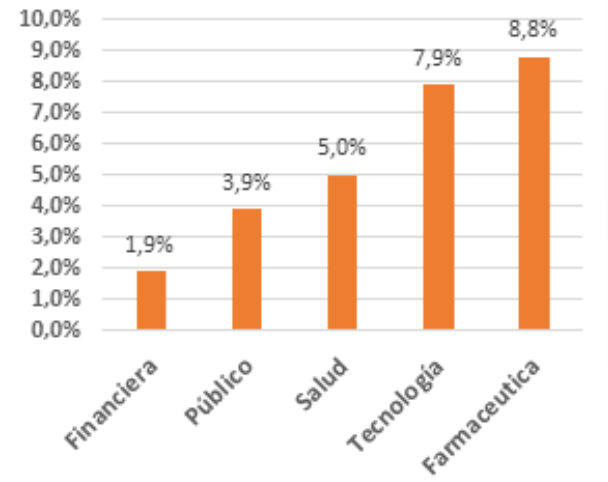
Fuente: KPMG, 2019, Consumer Loss Barometer
The economics of Trust. Elaboración propia.

Crecimiento del costo ante un incidente adverso de fuga de datos 2018-2019 (%)



Fuente: KPMG, 2019, Consumer Loss Barometer
The economics of Trust. Elaboración propia.

Incremento del costo por registro comprometido 2018-2019



Fuente: KPMG, 2019, Consumer Loss Barometer
The economics of Trust. Elaboración propia.

Con respecto a la retención de clientes tras una fuga de información, la industria financiera en una de las tres industrias con mayores retos junto a la industria de la salud y farmacéutica. En general, para todas las industrias la tasa gira alrededor del 3.9%; sin embargo, para la industria financiera esa tasa se encuentra en el 5.9%.

Adicionalmente, es muy importante para las empresas realizar seguimiento de eventos de fuga de información, ya que una implementación metódica de planes de monitoreo podrá impactar sustancialmente sus hojas de estado de Pérdidas Y Ganancias. De acuerdo con el reporte de IBM Security, el tiempo que le toma a una entidad financiera identificar que ha sufrido un incidente de fuga de información es de 177 días y el tiempo para contenerlo es de 56 días, con un tiempo total del incidente de 233 días. Lo que implica que, para la industria financiera, estos incidentes le pueden estar costando 4.56 millones de USD en promedio.

Las alternativas frente a este nuevo enemigo

Con respecto a los impactos de estos eventos en las cifras corporativas, es importante mencionar que, de acuerdo con el análisis del estado de automatización de la seguridad, la industria financiera aún tiene retos importantes. El 23% de la industria tiene completamente instalado, el 48% tiene parcialmente instalado y el 29% no cuenta con ninguna instalación[2].

Ahora bien, para estar preparados frente a incidentes de fuga de información, se necesita contar con una planeación ante eventos y un equipo de responsable del mismo. Estos deben estar en constante ejecución de auditorías que correspondan a probar los planes de respuesta ante incidentes y los protocolos de contención. Procedimiento, protocolos, capacitación continua e inversión en tecnología es vital. La industria no debe trabajar de manera aislada y debe implementar una extensión de su trabajo interno para ir de la mano con sus clientes, proveedores y aliados comerciales, en sus planes de prevención con el objetivo de extender la capacidad de reducción ante incidentes.

El instituto Privacy Rigths Clearinghouse, clasifica 8 eventos por medio de los cuales se materializa esta modalidad, los cuales pueden dar un marco a la gestión de la preparación ante incidentes y protocoles de seguridad:

- **Fraude relacionado con tarjeta:** Pueden presentarse tanto en tarjetas débito como en tarjetas crédito, en el momento de usar los canales de servicio, en los cuales por medio de dispositivos de escaneado (skimming) se obtiene los datos de la tarjeta.
- **Hackeos:** A través de operaciones de infección con código malicioso (malware).
- **Interna:** Cuando un empleado, contratista o cliente que puede tener acceso a dicha información la roba y la hace pública o la vende.
- **Perdida Física:** cuando los documentos en papel (físicos) que contienen dicha información son robados, erróneamente descartados o extraviados por falta de protocolos de archivo o seguridad en la manipulación de los mismo.
- **Perdida electrónica:** cuando los dispositivos dispuestos (Computadores, teléfonos, memorias, CD, discos extraíbles, cinta de datos, entre otros) para el trabajo son robados, descartados erróneamente o extraviados.
- **Toma de servidores:** Generado a raíz de una inadecuada gestión y administración de accesos.
- **Divulgación indebida:** Cuando de manera involuntaria se comparte por medio físico o electrónico, o se publica en línea, información que es de carácter confidencial.
- **Desconocido:** Cuando dicha información es expuesta, pero no se cuenta con información suficiente para rastrear el medio por el cual se ha dado el incidente.

2. Instalación del estado de automatización de la seguridad.

Los incidentes de fuga de información bajo sus distintas modalidades, quizás es de los temas de mayor importancia para el sector financiero. La banca por supuesto al manejar recursos del público, y tener la responsabilidad de administrar los datos personales de sus clientes, tiene un reto permanente para custodiar esos datos. En FELABAN siempre hemos considerado que una de las piedras angulares de dicho proceso es mediante la cooperación entre todos los jugadores involucrados. El gremio debe aglutinarse en torno a las mejores prácticas, el compartir información, y buscar en conjunto soluciones que combatan enemigos que no respetan sectores, ni fronteras. Hoy más que nunca es clave cerrar filas para no bajar la guardia ante las mutantes contingencias que este desafío implica.

Nota: Finalmente, para contextualizar los impactos de incidentes de fuga de información, dejamos casos de ejemplos de grandes fugas de información a entidades financieras a manera de Anexo

Bibliografía recomendada sobre el tema

Norton, What is Data Breach?, en: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

Forbes, What is a Data Breach?, Feb 2019, en: https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#eb209e414bbe

Kaspersky, What Is a Data Breach?, en: https://usa.kaspersky.com/resource-center/definitions/data-breach

KPMG, Consumer los Barometer The economics of trust, 2019, en: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/consumer-loss-barometer-2019.pdf

IBM Security, Costo f a Data Breach Report, 2019, en: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

Carnegie Endowment For International Peace, Timeline of Cyber Incidents Involving Financial Institutions, en: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide

South China Morning Post, Singapore, Malaysia credit card details dumped online in massive data breach, Marzo 2020, en: https://www.scmp.com/week-asia/article/3073848/singapore-malaysia-credit-card-details-dumped-online-massive-data-breach

Zdnet, Brazilian banking users exposed by 250GB data leak, Julio 2019, en: https://www.zdnet.com/article/brazilian-banking-users-exposed-by-250gb-data-leak/

-CNN, A hacker gained access to 100 million Capital One credit card applications and accounts, Julio 2019, en: https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

BBC, HSBC bank confirms US data breach, Noviembre 2018, en: https://www.bbc.com/news/technology-46117963

Forbes, Click2Gov Breaches Show The Power Of Zero Days, Diciembre 2018, en: https://www.forbes.com/sites/taylorarmerding/2018/12/21/click2gov-breaches-show-the-power-of-zero-days/#2700213b7e2e

CNBC, Equifax to pay $700 million for massive data breach. Here's what you need to know about getting a cut, Julio 2019, en: https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html

The Guardina, JP Morgan Chase reveals massive data breach affecting 76m households, octubre 2014, en: https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach

Forbes, Citigroup Data Breach: A Lesson and Warning For All, Junio 2011, en: https://www.forbes.com/sites/ilanagreene/2011/06/13/citigroup-data-breach-a-lesson-and-warning-for-all/#5ec393094817

SECRETARÍA GENERAL DE FELABAN

GIORGIO TRETTENERO CASTRO
Secretario General
gtrettenero@felaban.com

JORGE ARTURO SAZA G.
Director Económico
jsaza@felaban.com

DANIEL JUVINAO
Director Concentrador de Fraudes Regional y
Proyectos especiales
djuvinao@felaban.com

LAURA M. GORDILLO V.
Directora Adjunta Concentrador de Fraudes Regional
lgordillo@felaban.com

ADRIANA RODRÍGUEZ
Diseñadora Gráfica
arodriguez@felaban.com

FIC FRAUD INFORMATION CONTROL by FELABAN

FELABAN FEDERACION LATINOAMERICANA DE BANCOS
55 AÑOS 1965 - 2020

siganos en:

https://www.felaban.net
https://cfr.felaban.net

Casos de ejemplos de grandes fugas de información a entidades financieras

FECHA 1er Reporte de la fuga de información	NOMBRE ENTIDAD	MÉTODO Y TIPO	DATOS DEL INCIDENTE
2020- 6 de marzo	Sucursal de tarjetas de crédito de bancos del Sudeste asiático	Método desconocido Tipo: Fuga de Información	200.000 datos de tarjetas de crédito de bancos de Singapur, Malasia, filipinas, vietnam, Indonesia y Tailandia fueron robadas y publicadas en internet. Incluyendo los datos de número de la tarjeta, código de verificación y pin (para algunas entidades contraseña numérica de un solo uso). Uno de los bancos afectados, confirmó que sus sistemas no tuvieron incidentes y que los datos fueron obtenidos de otras fuentes.
2019 25 de Julio	Banco Pan	Método desconocido Tipo: Fuga de Información	250 gigas de información personal y financiera de la entidad financiera de Brasil Banco Pan, fue expuesta online. El banco aseguró que la información fue comprometida a través de uno de sus socios comerciales, la cual contenía tarjetas de identificación, documentos de confirmación de lugar de residencia y formatos de solicitud de servicios con información personal.
2019 29 de Julio	Capital ONE	Método: Hackeo Tipo: Fuga de Información	La entidad anuncio que sufrió un ataque que comprometió las aplicaciones de las tarjetas de crédito de alrededor de 100 millones de sus aplicantes. La información contenía, nombres, fechas de nacimiento, puntajes de crédito, información de contacto, y los datos de número de identificación nacional de estados unidos y Canadá. La información se encontraba depositada en los servidores de Amazon web servicies y fue obtenida tras un ataque de un hacker.
2018 6 de noviembre	Sucursal HSBC EEUU	Método: Hackeo Tipo: Fuga de Información	HSBC reportó que hackers obtuvieron acceso a datos que incluían nombres, direcciones, número de teléfono y datos de cuentas. No se confirmó el número exacto del impacto del evento, pero se estimó que menos de 1% de las cuentas online estuvieron comprometidas
2018 18 de diciembre	Portal de Pagos del Gobierno de EEUU	Método: Hackeo Tipo: Fuga de Información	El portar Click2Gov fue víctima, generando una exposición de datos personales, incluyendo datos de tarjeta de crédito, credenciales de acceso de usuarios de 40 estados y de dichos datos, fue detectada la venta en la Dark Web de los datos de las tarjetas de 10 Libras. Una empresa de consultoría descubrió además de la venta en la Dark Web, que los datos comprometidos fueron de aproximadamente 294.929 resultando en un impacto de 1.7 millones de dólares de ganancias para los ejecutores de dicho evento.

Casos de ejemplos de grandes fugas de información a entidades financieras

FECHA 1er Reporte de la fuga de información	NOMBRE ENTIDAD	MÉTODO Y TIPO	DATOS DEL INCIDENTE
2017 de septiembre	Equifax	Método Interna Tipo: Fuga de Información	La empresa reportó que fueron comprometidos 150 millones de datos de sus clientes, entre los cuales se incluía datos como fecha de nacimiento, y cerca de 12.000 número de identificación nacional. El evento fue materializado gracias a un error en la aplicación web apache struts, la cual la compañía no reparó. Los delincuentes escanearon las vulnerabilidades de y pudieron obtener acceso a la aplicación, un portal online en el que tras meses de están dentro de las redes, encontraron bases de datos con varios usuarios y contraseñas sin encriptar. El grupo Equifax, reportó haber invertido cerca de 439 millones en la administración del incidente de perdida de información.
2014 de Octubre	JP Morgan	Método: Hackeo Tipo: Fuga de Información	La compañía JP Morgan Chase, reportó haber tenido una fuga de información, que contenía información de cuentas y direcciones de residencia de 83 millones de clientes. Estos datos fueron expuestos, luego que criminales robaran las credenciales de acceso de un empleado de la compañía. El incidente fue logrado dado que un servidor de un solo factor de autenticación no había sido actualizado. Otras entidades como Dow Jones, Fidelity y E*Tarde también fueron atacadas. Las autoridades de los estados unidos concluyeron que estos datos fueron usados posteriormente es fraudes de seguros, lavado de dinero, fraude con tarjeta de crédito y fraude en compra de fármacos. En 2017 fue capturado una persona que se acogió a los cargos, relacionado a procesamiento de fondos a través de coin.mx una plataforma de cambio de bitcoin sin licencia.
2011 8 de Junio	Citigroup	Método: Interna Tipo: Fuga de Información	360.000 datos de tarjetas fueron expuestos, después de que criminales descubrieran una vulnerabilidad en la URL, que permitía saltar entre cuentas cambiando detalles pequeños de la dirección de la página web. Los criminales crearon un método para que esta acción se repitiera miles de veces para obtener información de contacto, dicha vulnerabilidad se encontraba latente desde 2008.