UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS ECONOMICAS Y FINANCIERAS

CARRERA DE CONTADURIA PÚBLICA

INSTITUTO DE INVESTIGACION DE CIENCIAS CONTABLES Y FINANCIERAS Y AUDITORIA

UNIDAD DE POSTGRADO

MONOGRAFIA

"DIPLOMADO EN AUDITORIA FORENSE"

TEMA: AUDITORIA FORENSE SOBRE TARJETAS CLONADAS

CASO: BANCO UNION

Postulante: ROSAISELA ARUQUIPA MACHICADO

Docente: DR. PABLO ARANDA MANRIQUE

La Paz, 2019

Bolivia

DEDICATORIA

Inicialmente deseo dedicarle este trabajo especial a todas las personas que siempre creyeron en mi capacidad, capacidad que tenemos todos, es grato saber la fuerza y determinación que poseemos cuando queremos alcanzar algo.

A mis padres la fortuna más grande es tenerlos conmigo y el tesoro más valioso son todos y cada uno de los valores que me inculcaron.

AGRADECIMIENTOS

Le damos gracias a Dios por permitirnos concluir esta etapa, por darnos la paciencia y la voluntad y a mi familia por su apoyo incondicional, por sus consejos.

Índice

1 Introducción

Actualmente en Bolivia existen normas informáticas. La norma madre es la Ley N° 164 de Telecomunicaciones, que regula el comercio electrónico, la firma digital, el gobierno electrónico, la comunicación de datos transfronterizos.

El Código Penal tipifica la Manipulación Informática artículo 363 bis y la Alteración, acceso y uso indebido de datos informáticos 363 ter. como delito.

Otro delito que se tiene tipificado es el acoso cibernético. Esta es una nueva figura legal que ha sido incluida en el Código Niño, Niña Adolescente, aprobado el 2015 en la Asamblea Legislativa Plurinacional, dice. La pena para quienes incurran en este delito será de entre cuatro y ochos años de privación de libertad.

Existen otros delitos informáticos que son las formas más frecuentes en la actualidad; es decir, formas delincuenciales cometidas utilizando medios informáticos ,así como el robo de información, suplantación de identidad, difamación, injurias o calumnias por internet y pornografía.

Las redes sociales son motivo de tanta discusión, su regulación tendrá que ver con el Derecho Informático, nueva rama en el ámbito legal. Si acaso se logra esa medida, deberá ser analizada con moral y ética, valores que hoy pocos tienen. Derecho informático es el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información.

El concepto que engloba es el de: Sociedad de la Información, en la cual la creación, la distribución y la manipulación de la información forman parte

importante de las actividades culturales y económicas, convirtiéndose en bienes intangibles altamente valorados. La Sociedad de la Información surge a partir del desarrollo tecnológico, en una relación dialéctica de mutua alimentación la cual potencia el desarrollo tecnológico, lo cual acelera el avance de la sociedad de la información.

El concepto de Derecho Informático surge, entonces, a partir de los conceptos de Tecnología de la Información y Sociedad de la Información, que son antecedentes identificadores de ese Derecho, cuyas fuentes tienen particularidades originadas en el vertiginoso cambio inherente al ámbito tecnológico.

El objeto de estudio del Derecho Informático es propio, aunque por el momento no necesariamente exclusivo. Esto se debe a que muchos aspectos abarcados por el Derecho Informático son abordados hoy por el Derecho Penal, Civil y Comercial, debido a la falta de legislación que contemple las particularidades que la Sociedad de la información implica. Es decir, la falta de plena autonomía en su objeto obedece más a la falta de legislación específica.

Las nuevas Tecnologías de la Información y Comunicación, por parte de los investigadores que atienden los delitos cometidos por la vía informática, retardan los procesos y muchas veces pone en riesgo la integridad de las víctimas. Es necesario expertos en Derecho Informático y nuevas tecnologías.

Es también conocido como skimming. Los delincuentes que se dedican a esto utilizan diferentes tipos de dispositivos electrónicos que le ayudan a clonar de las tarjetas.

El problema es que los dueños de las tarjetas de crédito o débito no se dan cuenta de esto hasta que les llega el estado de cuenta o cuando van a comprar algo en

una tienda o por internet con su tarjeta y le dicen que su tarjeta está al límite o se la rechazan. Otro gran problema es que esto de la clonación de tarjetas puede producir Robo de Identidad.

2. Planteamiento del problema

Dentro del sector financiero las Tarjetas de Débito o Crédito son un producto de mayor impacto para los usuarios y/o consumidores, ya que es una modalidad de dinero plástico y cuenta con varias ventajas a la hora del manejo y el riesgo ante el fraude o robo de las mismas, sin embargo se han venido presentado diferentes casos de corrupción o problemáticas en la clonación de estos, debido a que en su razón de ser esta fundamentalmente el cuidado y protección de la información financiera de todos y cada uno de sus usuarios.

Ante estas nuevas modalidades empleadas por los delincuentes que llegan a robar datos de tarjetas protegidas con chip y pin, es de gran importancia entender cómo operan y qué se puede hacer para no caer en sus redes.

2.1 Formulación del problema

¿Cómo se puede detectar que una tarjeta de débito sea clonada o una cuenta bancaria sea robada aún cuando actualmente existen medidas de seguridad, leyes e información?

3 Objetivos

Ante esta amenaza financiera, las entidades bancarias comenzaron a implementar medidas tales como la utilización de un pin y chip en las tarjetas, para así dejar

atrás la banda magnética, no obstante, el crimen también se ha transformado entonces se plantea lo siguiente:

Implementar estrategias que contrarresten el modus operandi y disminuyan los robos y víctimas mediante la difusión de la educación digital.

a. Objetivos Específicos

- Implementar una educación bancaria digital a toda la población en general.
- Dar a conocer los distintos modus operandis que existen y se han descubierto en la clonación de tarjetas.
- Proponer normas o estrategias para sancionar a los perpetradores.
- Crear más medidas de seguridad que contrarresten este tipo de delitos.

4 Justificación:

a. Metodológica

La elaboración y aplicación de estas estrategias indaga mediante métodos científicos, situaciones que pueden ser investigadas por la auditoría forense, una vez que se demuestra su validez y confiabilidad podrán ser utilizados para la prevención de estos delitos.

b. Académica

Dar a conocer información de la investigación porque podría servir para incentivar a los estudiantes la investigación y entre los alumnos y los docentes. Al mismo tiempo, podría ser utilizado para interaccionar con la población en general

c. Práctica

Esta investigación se realiza porque existe la necesidad de mejorar las medidas de seguridad en caso de las cuentas bancarias. Estas actualmente son parte necesaria de la vida de una persona es necesario saber todo acerca del manejo y prevenciones.

La Auditoría Forense Preventiva está orientada a proporcionar evaluaciones o asesoramiento a diferentes organizaciones de características públicas y privadas respecto de su capacidad para disuadir, prevenir, detectar y proceder frente a diferentes acciones de fraude. En la investigación desarrollada acerca de este caso sobre las tarjetas clonadas estas nos permiten distinguir con claridad el modus operandi que hoy en día se utiliza en robo de cuentas bancarias. Esto permitiría no solo aumentar la eficiencia en relación a la prevención como también en la enseñanza a la población en general.

5 Marco teórico/conceptual

a. Antecedentes de Tarjetas de Débito en Bolivia

En Bolivia existen más de 3 millones de tarjetas de débito y 4.753 puntos de atención financiera entre agencias, cajeros automáticos y otros, hasta agosto del 2015 (según la ASFI), se registró un crecimiento del 38,3% respecto al 2011, este aumento en el uso de las tarjetas bancarias se enmarca en la banca electrónica y las compras por Internet, que desde el 2014 viene realizando transferencias electrónicas con un crecimiento de 20% anual que ya superan hasta cuatro veces el PIB del país. En el país las tarjetas son un medio de pago poco usado, a pesar de contar con medidas de seguridad como la implementación de tarjetas con chip.

Las tarjetas de débito se encuentran habilitadas para comprar bienes y servicios en Internet. (Correo del Sur, 2015)

Las tarjetas de débito del Banco Nacional de Bolivia, Banco Mercantil Santa Cruz, Banco Económico, Banco BCP de Bolivia sirven como tarjetas de descuentos en comercios asociados a los mencionados bancos. Todos los cajeros automáticos están afiliadas a las redes internacionales Cirrus de MASTERCARD y Plus de VISA. Todas las terminales punto de venta y tarjetas de débito están afiliadas a las redes internacionales MASTERCARD y VISA.

Hasta agosto de la presente gestión el ente regulador registró 2.929.033 tarjetas de débito y 102.235 tarjetas de crédito, un crecimiento de 38,3% respecto a los datos registrados en 2011 cuando se contabilizaron en total 2.191.442 de tarjetas. (El día, 2015)

La cantidad de tarjetas registradas (3.031.268) respecto al número de cuentas de depósitos abiertas (8.489.134), hasta septiembre, representa el 35,7%. (Correo del Sur, 2017)

Las tarjetas de crédito, además de constituir un medio de pago, son también una forma de financiación, ya que permiten hacer compras sin la obligación de desembolsar la totalidad del dinero en el acto y con la posibilidad de devolverlo en varios plazos.

El uso de las tarjetas bancarias se enmarca en la llamada banca electrónica que en 2014 procesó 14,5 millones de transacciones por Bs776 mil millones, aproximadamente cuatro veces el PIB del país. Según el Banco Central de Bolivia

(BCB), las transferencias electrónicas registran un crecimiento de 20% anual. (Justiniano, 2017)

Los bancos pueden utilizar toda la tecnología que tienen disponible para la seguridad de sus clientes pero si los usuarios no están enterados de estos tipos de robos y presentan descuido con sus claves no tendrían derecho a reclamación alguna.

Figura 1 de Tarjetas de débito Actuales

Fuente: Correo del Sur, 2015

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable a través de vías informáticas tiene como objetivo dañar por medios electrónicos y redes de Internet. Existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la: Teoría del delito, por lo cual se definen como abusos informáticos 1 y parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático.

Los delitos informáticos son aquellas actividades ilícitas que: Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito). (Egocity, 2016)

Las formas en las que los delincuentes causan daños, provocan pérdidas o impiden el uso de sistemas como en nuestro caso un cajero automático.

Otra modalidad conocida de clonación se da por medio de la instalación de un dispositivo sobre el lector del cajero automático, con el cual crean un lector falso para robar sus datos. Una vez consiguen la información, la graban en una tarjeta nueva y obtienen su contraseña por medio de cámaras que instalan en los cajeros o por una persona que simula ser un cliente del cajero y observa cuando la víctima digita la clave. (Banco procredit, 2018, página 34)

Figura 2 Aparato mediante el cual almacena datos de la tarjeta de débito.

Fuente: La razón, 2018

5.2 Tipos de Clonación

a) Un centro falso de procesamiento

Este método puede usarse si un atacante es capaz de acceder al cable que conecta el cajero con la red. Un hacker desconecta el cajero de la red del banco y luego lo conecta a un aparato que actúa como un centro falso de procesamiento.

b) El ataque de la caja negra

Como en el método anteriormente descrito, el atacante obtiene la clave del bastidor del cajero y pone la máquina en modo de mantenimiento. Entonces, el hacker conecta la llamada caja negra al puerto USB expuesto. Una caja negra es un dispositivo que permite al hacker controlar el cajón del dinero.

Mientras el delincuente altera el cajero, la pantalla muestra un mensaje que dice en mantenimiento o fuera de servicio, aunque, en realidad, es posible sacar dinero de este. Además, la caja negra puede ser controlada de forma inalámbrica con un Smartphone. Un hacker solamente tiene que pulsar un botón en la pantalla para sacar dinero en metálico y deshacerse de la caja negra para esconder las pruebas.

c) Un ataque malware

Hay dos formas de infectar un cajero con malware: insertando un dispositivo USB con malware (eso conlleva tener la clave para abrir el bastidor del cajero) o infectando la máquina de forma remota, todo tras haber comprometido la red del banco.

Si el cajero no está protegido contra el malware y no emplea listas blancas, un hacker puede hacer que el malware envíe comandos al cajero y que este expenda dinero. El ataque podría repetirse hasta que el dinero del cajero se agote.

Por fortuna, no todos los cajeros se pueden hackear. Los ataques descritos anteriormente son posibles solo si algo no está bien configurado. Podría ser el caso de, por ejemplo, “Una red de banco no segmentada o de un cajero que no necesite una autenticación cuando el software intercambia datos con el hardware, o no haya listas blancas para las aplicaciones, o el cable de red esté al alcance del atacante”. (Hugo Franco, 2017, pagina1)

Por desgracia, este tipo de problemas son muy comunes. Por ejemplo, permiten a un hacker infectar una serie de cajeros con el troyano Tyupkin. Los expertos de Kaspersky Lab están siempre disponibles para ayudar a los bancos a solucionar este tipo de problemas: se ofrece servicios de consultoría o estudiar la infraestructura del banco mediante el análisis de su resistencia a los ataques. (Franco, 2017, pagina1)

5.3 Caso: Tarjetas Clonadas Banco Unión

Para poder entender más este tipo de casos se puede mencionar el siguiente caso:

El Banco Unión recibió 25 denuncias de clonación de tarjetas de débito y crédito, pero anunció que analiza el reintegro del dinero sustraído a sus clientes debido a que la mayoría contaba con seguro contra robo.

“La gerente de la entidad financiera, Marcia Villarroel, a tiempo de confirmar las quejas informó que la entidad evalúa cada una de los mismos casos por caso.

Más del 80% de los clientes tiene su seguro y, por tanto, se les va a cubrir, señaló en declaraciones desde Santa Cruz.” (Asoban, 2011, página 2)

“De acuerdo a la Asociación de Bancos Privados de Bolivia - Asoban la clonación de las tarjetas no se realizó en los cajeros automáticos, sino en los diferentes sitios habilitados para realizar transacciones.” (Asoban, 2011, página 2)

Se conoce que para efectuar la sustracción del dinero, los delincuentes utilizan aparatos que leen la banda magnética de las tarjetas en las máquinas de restaurantes, gasolineras y otros.
Tanto la ASFI como Asoban recomiendan que los usuarios renueven constantemente el número PIN para evitar robos, además de evitar la manipulación de las tarjetas por personas ajenas.

También memorizar el código PIN y evitar su anotación en papeles o el teléfono celular y revisar periódicamente las cuentas bancarias para vigilar que no existan consumos que hayan sido realizados.

Asoban anunció que para evitar mayores fraudes iniciará una campaña de prevención a nivel nacional, de modo que los usuarios del sistema financiero adopten todas las medidas de seguridad y recomendaciones.

5.4 Acceso a tarjetas de crédito en los últimos 7 años en Bolivia

“Hasta marzo de este año, en el país fueron contabilizados 6.235 puntos de atención financiera, de los cuales, 3.028 son cajeros automáticos y 3.157 son sucursales, agencias y otros. “En los primeros seis meses de 2015 hubo un 50%

más de denuncias por delitos vinculados al uso fraudulento de tarjetas que en el mismo periodo en 2014”. (Guarachi, 2018, página 3)

La clonación de tarjetas de crédito y débito en Bolivia puso en alerta a algunas entidades bancarias. Una de éstas es el Banco Mercantil Santa Cruz, que asumió como medida el cambio inmediato de la tarjeta del cliente cuando se verifica que es susceptible a ser reproducida. El gerente de Marketing del Banco Mercantil Santa Cruz, Sergio Unzueta, explicó que si bien las clonaciones de tarjetas de crédito se hacen más frecuentes en algunas épocas del año, la entidad está en constante actualización tecnológica para evitar este delito. “Hay infinidad de formas de clonación y para ello lo que se realiza es mantenernos siempre informados para compartir esta información con otros bancos y estar atentos con la idea de combatir este delito”, dijo Unzueta.

Figura 3. Diversos tipos de tarjetas de débito

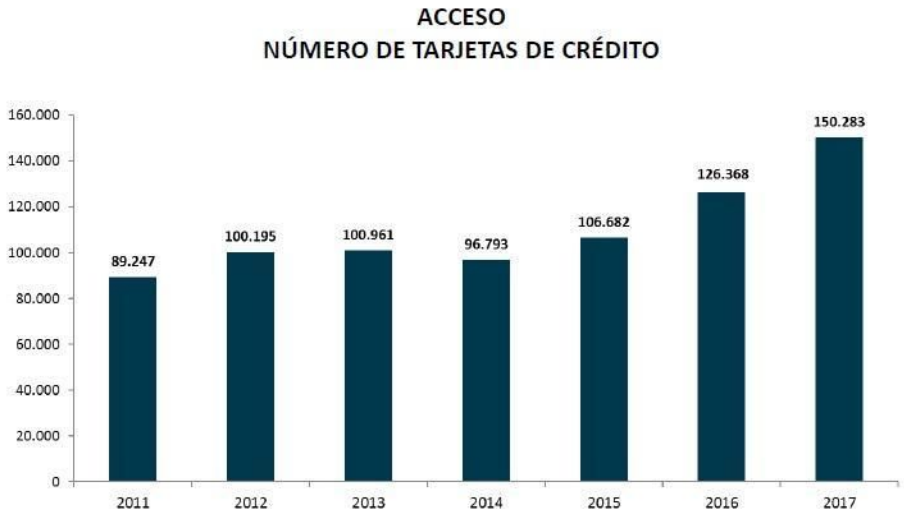
Fuente: Rojas, 2018

“El uso de las tarjetas de crédito fue incrementándose progresivamente desde 2011 hasta 2017 en el país. Durante ese tiempo, según datos de la Autoridad de Supervisión del Sistema Financiero – ASFI la cantidad de estas tarjetas emitidas subió de 89.247 en 2011 a 150.283 en 2017, lo que representa un incremento del 68,3%.El acceso al también llamado dinero de plástico no fue muy usual en el país entre 2011 a 2013, ya que durante ese periodo solamente fueron registradas 89.247 de estos documentos a 100.961, pero en 2014 hubo un descenso de 96.793 tarjetas”. (Guarachi, 2018, pagina1)

La tarjeta de crédito es un medio de pago emitido por una entidad financiera que le permite al usuario pagar en la mayoría de tiendas o establecimientos comerciales, realizar compras y disponer de dinero en efectivo cuando se necesite.

Desde 2014, la situación volvió a mejorar y se incrementó su acceso a 96.793; en 2015, subió a 106.682; en 2016 llegó a 126.368 y el pasado año, el ente emisor reportó un significativo incremento de 150.283 tarjetas emitidas. (Guarachi, 2018)

Figura 4.Uso de Tarjetas de débito



Fuente: Instituto Nacional de Estadística, 2013

“En el caso de las tarjetas de débito, se registró un ascenso desde 2011 con 2.102.195 personas que acceden a este documento a 2017 con 4.155.675, lo que significa un incremento del 97,6%”. (Guarachi, 2018, página 1)

En Bolivia, hasta marzo de este año, fueron contabilizados 6.235 puntos de atención financiera, de los cuales, 3.028 son cajeros automáticos y 3.157 son sucursales, agencias y otros.

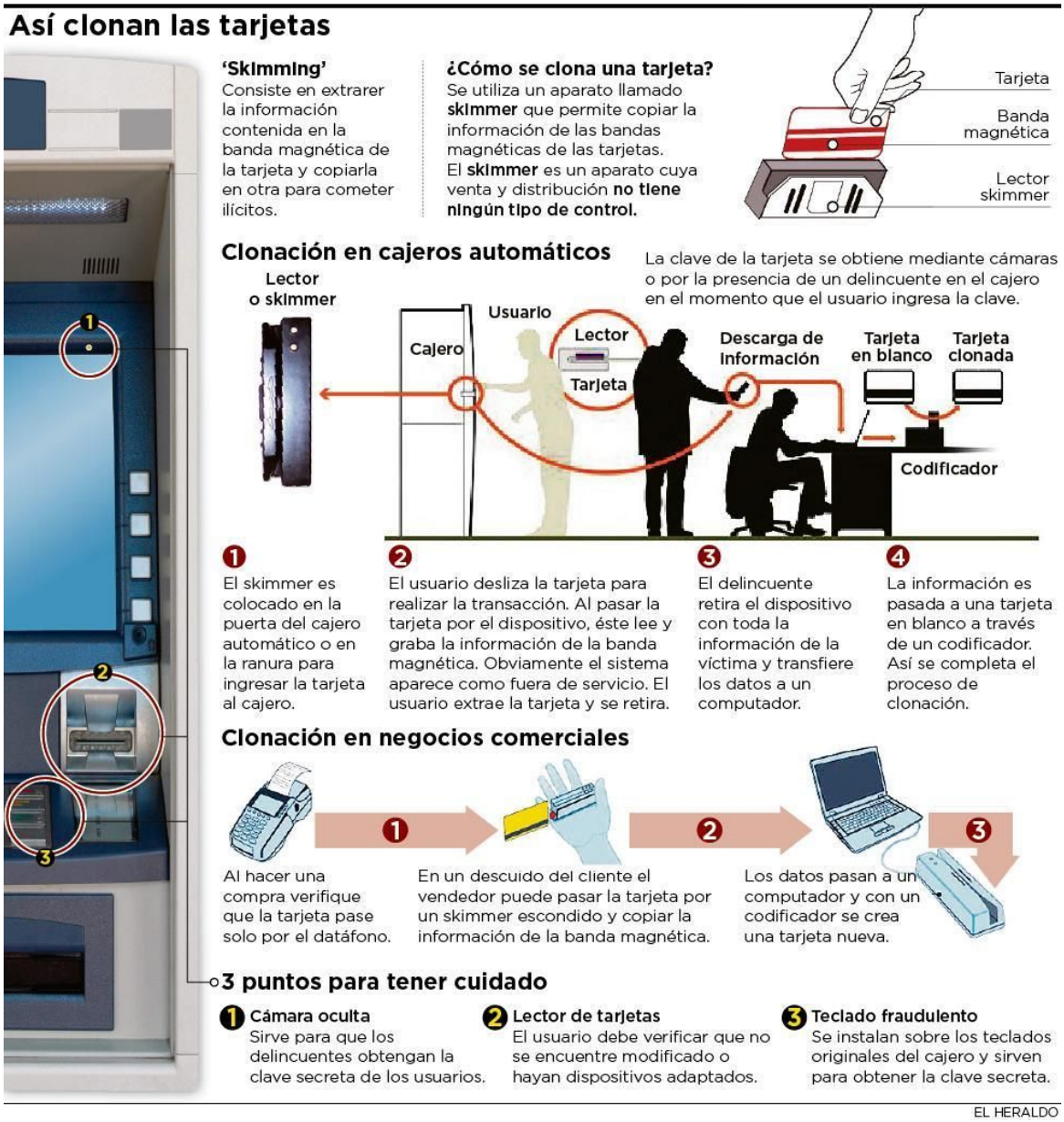
En 2017, la Administradora de Tarjetas de Crédito – ATC- Red Enlace reveló que solo cinco de cada 100 tarjetas de débito que hay en el país se emplean para efectuar compras o pagar servicios en internet, transacciones que se realizan en especial en los rubros de hotelería, agencias de viaje, cines y aerolíneas.

Las tarjetas de crédito, además de constituir un medio de pago, son también una forma de financiación, ya que permiten hacer compras sin la obligación de desembolsar la totalidad del dinero en el acto y con la posibilidad de devolverlo en varios plazos.

Un caso reciente es sobre un ciudadano mexicano que , fue aprehendido acusado de haber violado el precinto que se colocó en el departamento que era objeto de investigación, donde según el propietario sospechaba que su tarjeta de débito fue clonada.

“El propietario de un inmueble denunció inicialmente que en su cuenta bancaria se registra el retiro de dinero y sospecha que su tarjeta de débito fue clonada”, dijo a los periodistas.Indicó que la FELCC y el Ministerio Público ampliaron la investigación por el delito de apropiación indebida de fondos financieros.El ciudadano guarda detención en celdas de la FELCC y en las próximas horas será imputado por el fiscal asignado al caso”. (Erbol, 2018)

Figura 5. Así le clonan las tarjetas bancarias.



Fuente: Finanzas Personales, 2017

5.5 Fraude de tarjetas en el mundo

“Datos de Nilson Report indican que las pérdidas mundiales por fraude con tarjetas se elevaron a más de US$21.000 millones en 2015, frente a los 8.000 millones de dólares registrados en 2010.Para 2020, se espera que la cifra llegue a los US$31.000 millones. En estos costos, se incluyen, entre otros gastos, los reembolsos que los bancos y las compañías de tarjetas de crédito hacen a los clientes defraudados, lo que incentiva a las empresas de este tipo a realizar importantes inversiones en tecnologías antifraude. La actual vulnerabilidad del popular método de pago con tarjetas de débito y crédito -que poseen un chip y un número pin- ha sido expuesta por investigadores de la Universidad de Cambridge. Los hallazgos, presentados este martes en una conferencia de criptografía en Leuven, Bélgica, muestran que las tarjetas aún pueden ser clonadas, a pesar de las promesas de los bancos que aseguran que los dispositivos están protegidos de cualquier amenaza. Según los expertos, la razón es la escasa implementación de métodos de criptografía. Por ello, acusan a las instituciones bancarias de ocultar información acerca de las debilidades del sistema. El chip y el pin lideran los procesos de identificación en las transacciones de débito y crédito, con más de 1.000 millones de usuarios en todo el mundo. Debido a la seguridad actual, en comparación con tecnología previas como la clonación de la banda magnética, los bancos se han vuelto más agresivos con los reclamos de compensación, dicen los investigadores”. (Buonaguidi, 2017,Página 1)

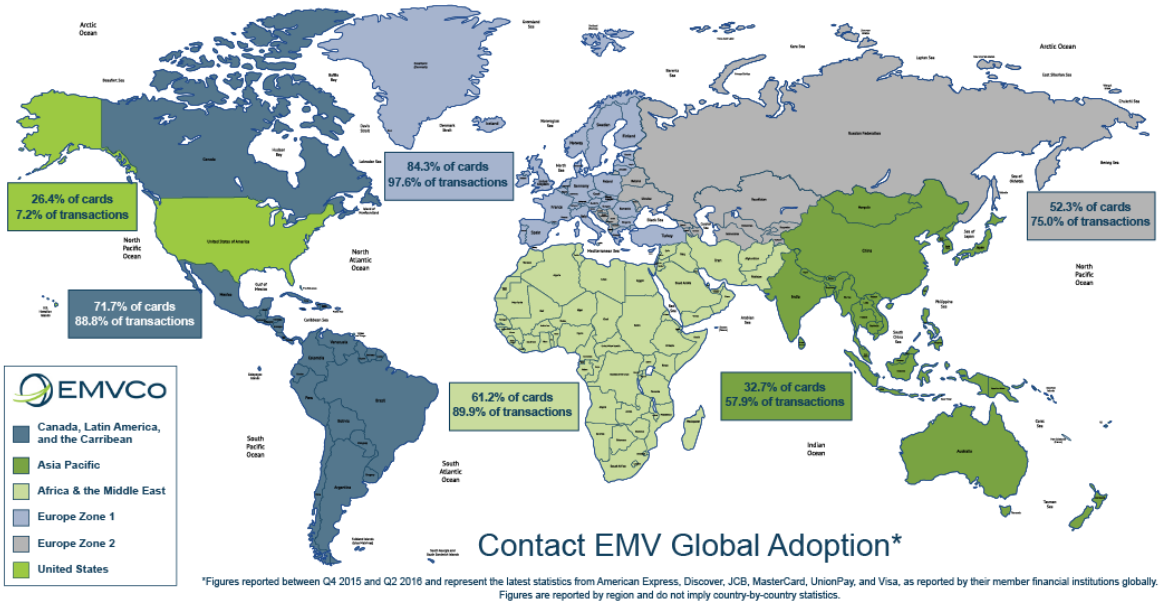
Sin embargo, el rechazo de los bancos a dar la compensación necesaria ha ayudado a que se realicen más investigaciones y se descubran otras vulnerabilidades.

Con el creciente uso de modos electrónicos de pago, en los últimos meses, en Uruguay se ha registrado un aumento de los casos de clonación de tarjetas de

débito o crédito a través de distintos sistemas. El más común hasta ahora se efectúa con dispositivos colocados en cajeros automáticos que permiten capturar los datos que están en el plástico y mirar con cámaras el número de PIN.

Actualmente, en muchos países, es difícil encontrarse con tarjetas bancarias que no cuenten a la vez con banda magnética y chip, cuando no son también contactless. El problema para dejar atrás la banda magnética, que como se han visto es un elemento totalmente inseguro, es que para ello todo el mundo tiene que adaptar sus cajeros, por el lado de los bancos, sus tarjetas y los datáfonos, por el lado de los comercios, para poder leer los chips.

Figura 6. Casos en el mundo



Fuente: Smith, 2018

Y por mucho que los bancos, tarjetas y tiendas alrededor puedan estar adaptados, se podría encontrar bancos y/o tiendas no adaptados o usuarios con tarjetas sin chip, por lo que mientras el chip no sea aceptado globalmente no pueden dejar atrás la banda magnética.

Los chips de las tarjetas con circuito integrado están cifrados y al menos de momento han demostrado ser seguros EMV es el nombre con el que se conoce a las tarjetas con circuito integrado, aunque dichas siglas únicamente responden a las compañías que establecieron dicho estándar Europay, Mastercard y Visa aunque posteriormente a ellas se han unido otras empresas.

Toda la información contenida en los chips de las nuevas tarjetas está protegida mediante el uso de algoritmos de cifrado como Triple-DES, SHA o RSA, que por lo menos hasta el momento han demostrado ser infranqueables, por lo que acceder al contenido del chip y duplicarlo debería ser imposible.

Figura 7. Terminal de Escaneo para clonación.

Fuente: Canedo, 2017

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) alertó sobre una nueva forma que utilizan los estafadores para clonar tarjetas en terminales de algunos comercios.

El modus operandi comienza cuando los estafadores se hacen pasar por personal de alguna de las instituciones financieras y envían mensajes a las empresas o pequeños comercios para informarles sobre una “actualización del sistema de la terminal punto de venta” (del ordenador, no del lector de tarjetas físico), para lo cual les solicitan acceso remoto a la terminal. Una vez que obtienen el acceso, los estafadores infectan la máquina a distancia.

De acuerdo con la Condusef, este tipo de fraude permite que los responsables consigan la siguiente información:

Datos personales del tarjetahabiente
Número de cuenta
Número de tarjeta
Fecha de vencimiento
Tipo de tarjeta

“Estos datos son cargados a una tarjeta conocida como ‘Tarjeta Paloma’ y toda vez que el malware permite manipular el proceso de verificación de la autenticidad del titular de la tarjeta, cualquier número puede ser considerado válido con NIP, pudiendo ser utilizada para realizar cualquier tipo de compra, ya sea en TPV (terminal punto de venta) o compras en línea”.(BBC, 2018, página 1)

Cómo evitar los intentos para clonar tarjetas en terminales

Luego de emitir la alerta, la Condusef llamó a todos los comercios que utilizan terminales punto de venta a estar alerta ante este tipo de llamadas de servicio de mantenimiento o de actualización que son fraudulentas y emitió las siguientes recomendaciones para los propietarios de establecimientos:

Verifica con la institución financiera las condiciones de uso de la Terminal Punto de Venta. Antes de permitir alguna actualización, contacta a la institución financiera.

5.6 Nuevas formas de realizar transacciones

Actualmente existen otras formas de realizar transacciones sin necesidad del hacer uso de las tarjetas que incluso prometen más seguridad.

Se puede mencionar un caso en el continente asiático específicamente China como se está dejando de lado esta forma de transacción.

En China han encontrado la forma de saltarse estas comisiones en su mayor parte, eliminar costes a los comercios, y permitir vivir con pagos móviles que van mucho más allá de lo que se conoce en España. Mientras que las personas estan acostumbrados a que los pagos móviles consisten en tener una copia virtual de la tarjeta física en nuestro smartphone, en el país asiático están yendo más allá con pagos mediante códigos QR, un sistema que ha cambiado por completo las transacciones comerciales en supermercados, gasolineras, taxis y cualquier tipo de establecimiento. Incluso para pagar facturas. En la mayoría de países del mundo, los pagos los componen el dinero en efectivo y una lista de entidades bancarias y partners para el dinero de plástico, con VISA y MasterCard a la

cabeza. En China apenas compiten Alipay y WeChat Pay, controlados por AliBaba -que viene a ser el Amazon chino- y Tencent Holdings -propietario de WeChat, el WhatsApp de China que va muchísimo más allá en cuanto a funciones. Apuntar con la cámara, tocar, confirmar. A eso se reduce el proceso de pago mediante QR en China. “El servicio de Alipay es gratuito para los usuarios menos frecuentes, a medida en que se van incorporando comisiones crecientes. Pero incluso la mayor de todas es más baja que la de PayPal, por ejemplo: un 1,2%. Las plataformas digitales de Alibaba y WeChat se han convertido en ecosistemas casi integrales donde sus usuarios realizan muchísimas acciones para las que quizás en occidente estan acostumbrados a usar varias apps por separado. Cada usuario tiene un QR único, también los comercios, y comunicándose entre ellos es como se completan los pagos. Bancos y proveedores de tarjetas de débito y crédito quedan fuera de una ecuación que se prevé al alza y sin visos de que sea ninguna moda”. (Lacort, 2018, pagina1)

Los que no cuentan con una de estas TPV únicamente deben tener el QR de su negocio impreso en un folio de papel cualquiera al que apuntan con la cámara los compradores para ejecutar el pago.

“No se necesita estar pendiente de si el establecimiento tiene TPV, o si este tiene NFC para pagar con el móvil, ni de si exige un pago mínimo: se asume que todo el mundo tiene un Smartphone”. (Durango, 2017, pagina1)

John Engen, de American Banker, escribió que los bancos a menudo se reducen a actores pasivos, en referencia al mismo concepto que a veces se usa para hablar de las operadoras en la era de las OTT's: han dejado de tener el control sobre lo que ocurre con sus clientes, limitándose a ser una intermediación suave que tiende a commodity.

Las víctimas de esta revolución móvil no se limitan a bancos y proveedores de tarjetas, el dinero en efectivo también va viendo cómo su uso se queda en

residual. El propio Engen explica que basta con ver una cola en un comercio para darse cuenta de cómo quien usa efectivo ralentiza muy notablemente el proceso.

Al otro lado del mundo, WhatsApp ya está experimentando con pagos vía QR en su beta. Si finalmente se integra en la app y se logra una buena experiencia de uso, se puede ver un panorama completamente distinto en España dentro de unos años, ya que nuestro país tiene una de las mayores penetraciones de uso de WhatsApp del mundo.

Otros, como India, tienen una penetración similar pero además usan WhatsApp para prácticamente todo: llamadas, videollamadas, contenido efímero ¿Será Facebook quien se lleve el premio del pago QR en occidente?

Figura 8 Códigos QR.

Fuente: Fuentes, 2017

> “Los canales digitales cada vez son más usados para hacer transacciones bancarias. Productos como la Sucursal Virtual o Ahorro a la Mano son preferidos por muchas personas por su flexibilidad y utilidad: los usuarios no dependen de los horarios de las sucursales, ni de su ubicación física para hacer sus movimientos financieros”. (Fuentes, 2017, página 57)

Como usuario bancario y víctima de este fraude usted cuenta con dos vías inmediatas,

La primera es acudir con urgencia a la entidad bancaria a la cual se encuentra afiliado y la segunda, consulta directamente con la Superintendencia Financiera en el departamento de protección al consumidor financiero, para que esas entidades empiecen con la investigación pertinente. Luego, es aconsejable que el usuario se dirija a la Policía Nacional para poner la denuncia (con la documentación que le proporcionó el banco) y así empezar una investigación paralela que puede ser dispendiosa y demorada.

La entidad bancaria después de conocer el caso por parte de sus clientes comienza la respectiva investigación donde determinan la culpabilidad del usuario como (descuido de s clave, ayuda de terceros en la transacción) o si por el contrario fue víctima de fraude.

Dependiendo del resultado de esta indagación los bancos reconocen parcial o totalmente el valor hurtado.

Los bancos pueden utilizar toda la tecnología que tienen disponible para la seguridad de sus clientes pero si los usuarios no están enterados de estos tipos de robos y presentan descuido con sus claves no tendrían derecho a reclamación alguna.

Para que exista un fraude en la clonación de tarjeta es necesario que se duplique información de la banda magnética y que se obtenga la clave, con estos datos se realiza el desfalco en la cuenta de la víctima.

“A pesar de esto estas tarjetas tiene un seguro todo riesgo donde cubren el uso indebido o utilización fraudulenta de la tarjeta generada por una tercera persona no autorizada, las personas por lo general no tienen conocimiento de este seguro y el uso que pueden darle en caso de ser víctimas de este delito aunque para que el banco asuma el seguro deben hacer la investigación correspondiente dentro de

los plazos estipulados y con la documentación requerida para este tipo de trámite". (Durango, 2017, página 17)

Particularmente, en cuanto a la clonación, los bancos han desarrollados medidas como:

1) Emisión de algunos tipos de tarjetas con tecnología EMV (conocida como tarjeta chip)

2) Instalación de dispositivos antiskimming en los cajeros (o ATM)

3) Instalación de cámaras en cajeros asociados con cada transacción.

4) Información en línea (a través de mensaje de texto o correo electrónico) sobre las transacciones realizadas.

5) Capacitaciones a establecimientos comerciales para el debido uso de las tarjetas en los datafonos.

6) Campañas comunicacionales a los clientes para que tomen las debidas precauciones en el momento de realizar sus transacciones. (Semana, 2012)

Si se tienen varias denuncias sobre un cajero en específico o algún establecimiento público donde informen un posible fraude los bancos abren una investigación para identificar cuál es el método utilizado en dicho suceso y tomar los correctivos necesarios para evitar esta fuga de información.

Al final con los resultados obtenidos en la investigación se da a conocer sobre quien recae la responsabilidad y cuáles son las medidas a tomar para restablecer lo perdido a los usuarios.

Por parte de la policía Nacional también se realizan ciertas recomendaciones para evitar ser víctima de este tipo de fraudes el cual se presenta en diferentes situaciones y modalidades.

En cajeros electrónicos

- Validar que no exista ningún aparato instalado en la ranura de ingreso de la tarjeta de crédito.
- Al realizar un pago con débito no perder de vista la tarjeta en ningún momento y validar que si sea la tarjeta con los datos propios.
- Nunca aceptar ayuda de extraños
- No confiar en la amabilidad de un desconocido al realizar una transacción
- En lo posible oculte la clave al digitarla
- Si detecta alguna anomalía informar a la entidad correspondiente o a la policía nacional

En restaurantes o estaciones de gasolina

- Realizar la operación de manera personal y no permitir que la realice un tercero.
- Cubrir el teclado del dispositivo al momento de digitar la clave.
- Estar alerta de que la tarjeta solo sea deslizada una vez por el dispositivo y verifique cuando la devuelvan que si sea la suya.
- No arroje a la basura los comprobantes de pago donde estén registrados los datos personales.

6 Marco Metodológico

La presente investigación tiene un enfoque Analítico, enfocado en un manejo descriptivo de las situaciones presentadas en casos de clonación de tarjetas, se desglosan los diferentes factores que intervienen en este delito, se pueden encontrar causas, naturaleza de la problemática presentada y por supuesto los efectos que tiene dicho indicador en la economía nacional.

6.1. Enfoque

Es exploratorio, porque anteriormente este tema se ha vuelto necesario de estudiar. Se hizo relación entre datos los casos acontecidos en los últimos años como creció el uso de este método de robo mediante la clonación de tarjetas.

6.2 Tipo de investigación

La investigación desarrollada es de tipo descriptivo, ya que, nuestro estudio realizado pretende conducir a la comprensión de un fenómeno como la clonación y el impacto generado en todos los usuarios, se busca encontrar las causas que lo generan orientados y la identificación y el análisis de variables independientes y sus resultados, tratando de llegar a hechos verificables en nuestra investigación.

6.3 Fuentes de investigación

Las fuentes principales de información se basaron en la web, Periódicos digitales, Casos que acontecieron los últimos años. También las normativas bolivianas actuales aunque de esta parte se destaca la necesidad de contar normas actuales acorde con la coyuntura actual porque existen muchos vacíos legales. Aunque se han creado instituciones como la ASFI para poder controlar a las entidades financieras estas todavía no ofrecen la seguridad que pueda evitar robos.

6.5 Instrumento de aplicación

El instrumento de búsqueda utilizado fueron principalmente las bases de datos de Asobancaria, artículos de diferentes revistas y periódicos a través de estos mecanismos de búsqueda se basa en un abogado con amplia trayectoria en el sector financiero y actual Defensor del Consumidor Financiero del Grupo Bancolombia.

7 Marco Práctico

¿Cómo evitar que una tarjeta de crédito sea clonada?

Primero hay que entender que, existen otras modalidades de robo y clonación de tarjeta utilizadas por los ciberdelincuentes. Según Kaspersky Lab, parte de las más utilizadas es la instalación de un virus en celulares, computadores y tabletas, este software malicioso recopila información de la víctima, como número de cuenta, claves y otros detalles necesarios para realizar una operación bancaria.

“En palabras más sencillas esto se traduce en un espía que vive dentro de los aparatos tecnológicos y que junta la información que registran los usuarios en canales financieros”. (Ojeda, 2018, pagina1)

Pero además se ha comprobado que los delincuentes también han logrado manipular canales de venta utilizados a nivel global, como por ejemplo los datáfonos, que también son comprometidos para recolectar información financiera de tarjetas crédito y débito.

En primer lugar seria estar al tanto de las notificaciones que los bancos envían a sus clientes, vía mensaje de texto o correo electrónico, para así detectar cualquier movimiento financiero que estén haciendo desde su cuenta y sin su

consentimiento. En este caso lo que el usuario puede hacer es reportar el problema y así evitar que el daño escale a un escenario mayor.

“Como segunda recomendación Pintoroli sugiere utilizar canales como AndroidPay o ApplePay, explica que estos medios de pago no revelan el número real de las tarjetas, sino que generan unos virtuales que son utilizados exclusivamente para la transacción que se haga en ese momento”. Diego (Ojeda, 2018, pagina1)

Con lo propuesto se logrará efectuar un análisis de los resultados que serán en base al cumplimiento de los métodos mencionados estos evitaran este tipo de robos y además las acciones inmediatas que se deberán tomar por parte de las personas afectadas y el Banco además de sancionar a las personas que recurren a este modus operandi de clonación de tarjetas para hurtar.

Para describir en forma más general que debería hacer un usuario de encontrarse en esa situación se menciona lo siguiente:

¿Qué se debe hacer para evitar que la tarjeta sea clonada?

A continuación, 7 consejos para hacer más difícil que algunas de las personas sean blanco de estos ladrones de cuello blanco.

a) Cambiar en forma periódica el PIN de la tarjeta e intentar no ir variando alternadamente dos diferentes.

b) No perder de vista la tarjeta cuando se realizan compras o transacciones de cualquier clase.

c) Cubrir con una mano cuando digita el PIN en un cajero automático o en un POS.

d) Al entrar a un cajero automático no permitir que personas se pongan al lado, de preferencia ingrese en forma solitaria. Tenga particular cuidado de tapar cuando digita el PIN en cajeros ubicados en lugares abiertos y con circulación de personas (estaciones de servicio, kioskos, etc.).

e) No recibir ni solicitar ayuda de extraños para realizar transacciones con tarjetas.

f) Revisar periódicamente el resumen de cuenta de la tarjeta o sus transacciones en la página web de su banco a fin de verificar la normalidad de las transacciones.

g) Cuando paga con tarjeta y esta sea sospechosa, es recomendable ingresar una clave errónea. De este modo, si la compra es aceptada, significa que la máquina fue adulterada y puede estar siendo víctima de una maniobra de clonación de tarjetas.

¿Qué hacer si se clonó una tarjeta?

Seguir 4 sencillos pasos:

a) Cancelar la tarjeta

Llamar al banco y reportar delito en cuanto una tarjeta sea clonada, para que la tarjeta sea cancelada, con esto se evita que los delincuentes realicen otros cargos.

b) Presentar la queja

Existe un plazo de 90 días naturales, contados a partir de la fecha de corte, o en su caso, de la fecha en que se efectuó el cargo no reconocido para presentar la

solicitud formal de reclamación. Se puede hacer directamente en la sucursal donde tienes tu cuenta, o bien, en la Unidad Especializada del banco, mediante escrito, correo electrónico o cualquier otro medio por el que se pueda comprobar la recepción.

c) Llenar el formato de aclaración

El banco proporcionará un formato de solicitud de aclaración, ya sea en sucursal o a través de su portal de internet. Es obligatorio al acusar con recibo la solicitud, indicando al menos un folio, la fecha y hora de recepción. Podrán pedir presentes una identificación oficial.

d) Una declaración de hechos

Tomar un tiempo y escribir con la mejor redacción que se pueda. Este documento se debes anexar al formato de aclaración y puede ser muy útil en la resolución a favor. Banco Mundial Interamericano (2018)

Figura 9. Seguridad en la nube

Fuente: Juan Maldonado, 2015

Otras medidas a tomar serían:

- Solicitar al banco cambio de tarjeta, por una con medidas de seguridad complementarias, como chip inteligente.
- Revisar frecuentemente los saldos de las cuentas.
- Si se detecta un consumo que no realizo, notificar al banco de inmediato.
- No compartir contraseñas y cambiarlas cada cierto tiempo.
- Cuando se realiza transacciones online, verificar que sean en sitios y comercios seguros.
- El banco nunca pedirá información personal o contraseñas.
- En caso que la tarjeta sea clonada se bloquearla lo más rápido.

Una buena práctica es utilizar una tarjeta separada al momento de hacer compras en línea, esto permitirá tener una mayor visibilidad del plástico para saber si está comprometido en uso de tiendas virtuales o comercios tradicionales.

También verificar la autenticidad del cajero y que esté en funcionamiento, y además cambiar constantemente las claves y que éstas no sean fáciles de averiguar.

Como prevención, que las ranuras estén libres. Tanto la de la puerta, como la del mismo cajero. En algunos casos es muy fácil descubrirlo.

Por otro lado, se aconseja que cuando se digite la clave secreta se tape con la mano, ya que en algunos dispensadores los delincuentes colocan cámaras para grabarlas.

En ese instante tu clave es captada en la micro cámara dentro del espacio del cajero.

“Además, se debe fijar en las personas que están alrededor al momento de realizar un giro; y después de realizarse, siempre se debe verificar el saldo luego de la operación. “Al ingresar al cajero hay que usar el cuerpo cubrir las acciones en la máquina, no hablar con nadie mientras realizas la operación e ingresar a sucursales de día, con iluminación y que posean cámaras instaladas por la empresa”. (Acuña , 2018 , pagina1)

Otros consejos son tapar con la otra mano el teclado al momento de tipear el PIN, para evitar cámaras; usar alertas móviles para detectar pagos no habituales con tarjetas (algunos bancos lo ofrecen); y evitar cajeros cuya estructura no sea la habitual, o que parezcan manipulados o dañados.

Para evitar que se repita el delito, la entidad identifica un punto geográfico en común en Bolivia en donde se hayan realizado transacciones con tarjetas de crédito que posteriormente fueron clonadas. Se cuantifican y se miden los tiempos en los cuales se utilizaron.

Luego de verificar la cantidad, el banco se comunica con los clientes para advertirles que sus tarjetas están propensas a ser clonadas.

En Bolivia es verdad que las telefónicas y la banca son las que más invierten en tecnología y gran parte de esa tecnología va destinada al campo de seguridad, porque es uno de los puntos más importantes al igual que el riesgo operacional. Pienso que la banca está tomando muchas precauciones y parte de esa estrategia es impulsar la seguridad. Es un importante punto para ellos para evitar clonaciones. De todo lo que se invierte en tecnología un 7 ó 8% va destinado a la seguridad.

8 Conclusiones

Se evidencia que los bancos en algunas ocasiones responden ante este tipo de situaciones no siempre son favorables para los clientes dado que como tal no se realiza directamente el fraude al banco sino al portador de la tarjeta motivo por el cual la investigación se puede hacer algo extensa y difícil de probar.

Es claro la falta de información y sensibilización para que todas las personas estén enteradas de los métodos de clonación que existen y cómo prevenirlos, ya que actualmente las personas solo se interesan por el caso cuando les ocurre un suceso de estos o a algún familiar o persona de su entorno.

A pesar de que las entidades financieras invierten dinero en la seguridad de sus productos en este caso las tarjetas de crédito los delincuentes siguen burlando dicha seguridad de una u otra manera, se deben crear estrategias que permitan la disminución de las clonaciones.

Quienes cometen este tipo de delitos no tienen ninguna especialidad técnica, ya que sólo le alcanza con conocer los pasos y repetirlos mecánicamente.

Hay gente que recluta las tarjetas, otros que las compran y otros que hasta arman negocios. Todo esto en un mercado ilegal.

De la presente investigación se llega a la conclusión de que es necesario un proceso de **actualización** en leyes y **educación** acordes con la globalización eso como **medida de prevención**, **sanciones, planes de contingencia** y crear alternativas para realizar transacciones más seguras.

9 Recomendaciones

Para evitar que ocurran este tipo de incidentes se debería tomar medidas de precaución y tener planes de contingencia, hacer una actualización constante sobre manejo de transacciones y mejorar la Implementación de las leyes acorde a la coyuntura actual.

También seguir los procedimientos y pedir asesoramiento ,que los bancos realicen campañas por medio de mensajes masivos a los mails , volantes, campañas en sus páginas web, información visible en las oficinas y difusión por medios televisivos donde se den recomendaciones acerca de cómo prevenir este delito.

Otra alternativa práctica es utilizar el pago móvil esta es una de las innovaciones más importantes en la convergencia de las novedades tecnológicas y su aplicación es comercial. Además, cada vez más plataformas lo permiten. Sin embargo, muchas personas no saben cómo funciona esta tecnología actualmente.

El historial de compras, la ubicación geográfica del cargo, cuál fue el negocio donde se hizo la compra y las cantidades gastadas son algunos factores que suelen utilizarse en los sistemas de detección de fraudes.

Si quiere saber cuáles son otras protecciones que el banco o empresa de tarjeta de crédito tienen disponibles para tu cuenta, entrar al sitio web y busca la sección de seguridad.

Los fraudes se cometen todo el año pero, debido a que este mes el Servicio de Rentas Internas de Estados Unidos está en la mente de muchas personas,

también debes estar alerta de las estafas relacionadas con los impuestos. El sitio IRS.gov tiene información sobre las trampas más recientes y cómo denunciarlas. Muchas instituciones financieras tienen algoritmos sofisticados y automatizados que detectan fraudes, los cuales puede encontrar señales de alguna actividad inusual en tu cuenta, a menudo antes de que la persona se percate.

Luego de constatarse el robo de cerca de medio millón de dólares con tarjetas clonadas a más de 600 clientes del sistema financiero en Bolivia, la Autoridad de Supervisión del Sistema Financiero (ASFI) obligó a los Bancos y entidades financieras a incluir el microchip en tarjetas de crédito y débito.Los operadores del sistema de intermediación financiera debieron hacer conocer a la ASFI el cronograma que tienen para la migración del sistema de banda magnética al sistema de microchip hasta el 31 de diciembre del año pasado.La directora de la entidad reguladora, Lenny Valdivia, explicó a Xinhua que a partir del 1 de marzo, las entidades del sistema de intermediación financiera ya no podrán emitir más tarjetas de débito o crédito con banda magnética, puesto que tienen plazo hasta diciembre de este año para proceder al cambio por las nuevas con chip."Actualmente debo decirlo con mucha satisfacción que todas las entidades del sistema de intermediación financiera han cumplido, porque a partir de noviembre están emitiendo para tarjetas de crédito, ya todas con el sistema de microchip", explicó la autoridad financiera.Datos de la ASFI señalan que en Bolivia existen 92.187 usuarios de tarjetas de crédito y más de 2,2 millones que tienen tarjeta de débito, efectivizando un total de 2 millones 367.735.El objetivo de migrar a tarjetas con chip es dar mayor seguridad y evitar la clonación de las tarjetas que contienen una banda magnética y que son mucho más susceptibles de ser clonadas.En Bolivia en los últimos años se masifican en el uso y la demanda de las tarjetas magnéticas para acceder a los servicios del sistema financiero y con ello las amenazas de los delitos informáticos.(La Razón, 2018, página A3)

10 BIBLIOGRAFÍA

- Angel Guarachi ,Informática Jurídica , Recuperado de 12 de abril de 2018 de http://www.informatica-juridica.com/legislacion/bolivia/

- Catalán, J. (2001). Fobia social y timidez. Recuperado el 21 de agosto de 2002, de http://www.cop.es/colegiados/A00512/timidez.html

- Credibanco. (S.F.). Credibanco. Obtenido de https://www.credibanco.com/credibanco/historia

- Decreto Supremo N° 21531, Régimen Complementario al Impuesto al Valor Agregado. Gaceta Oficial e Bolivia, ed. 1504, 28 de febrero de 1987.
- El tiempo (08 de marzo de 2016). Atento: así los delincuentes le pueden clonar sus tarjetas. El tiempo. Recuperado de http://www.eltiempo.com/archivo/documento/CMS-16531389

- El tiempo (27 de abril de 2016). La banca y aseguradoras, en alerta por estafas con pagos por internet. El tiempo. Recuperado http://www.eltiempo.com/archivo/documento/CMS-16574145

- Hannober, C. (2018) .Delitos informáticos carecen de atención oportuna y capaz. Recuperado el 13 de marzo de 2016, https://www.paginasiete.bo/sociedad/2016/3/13/delitos-informaticos-carecen-atencion-oportuna-capaz-89688.html

- Ley N° 1606, Modificaciones a la Ley N° 843. Gaceta Oficial de Bolivia, ed. 1863. Recuperado el 22 de diciembre de 1994de:http://www.gacetaoficialdebolivia.gob.bo http://www.oas.org/juridico/spanish/cyb_bol_codigo_penal.pdf

- La Tercera (1 de junio 2017) Medidas en caso de una clonación. https://www.latercera.com/noticia/conoce-las-medidas-debes-tomar-evitar-tus-tarjetas-sean-clonadas/

ANEXO I

CÓDIGO PENAL SEGÚN LEY N° 1768 DE MODIFICACIONES AL CÓDIGO PENAL

CAPÍTULO XI

DELITOS INFORMÁTICOS

ARTÍCULO 363 bis.- (MANIPULACIÓN INFORMÁTICA).- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa desesenta a doscientos días.

ARTÍCULO 363 ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

ANEXO II

ASFI - IMPLEMENTACIÓN DE TARJETAS CON CHIP EN BOLIVIA (ESTÁNDAR EMV)

La recurrencia de denuncias y reclamos atendidos en los últimos años sobre hechos delictivos acontecidos en el país relacionados con la presunta sustracción de dinero de cajeros automáticos por clonación de tarjetas de débito y crédito de clientes de las entidades de intermediación financiera, se presentaron en una alta intensidad en los primeros 4 meses del año 2011, periodo en el cual se registraron 1,064 reclamos relacionados a fraudes con tarjetas de débito y crédito, en los diferentes Puntos de Reclamo (PR). Con el propósito de precautelar la seguridad de las operaciones de los clientes esta Autoridad de Supervisión, efectuó un análisis sobre la problemática relacionada a las tarjetas de pago y observó que los delitos informáticos no eran un fenómeno aislado que se presentaba en Bolivia, sino una consecuencia de la migración de organizaciones criminales especializadas en fraude informático, cuyo modus operandi consistía en trasladarse hacia los países más vulnerables en temas de seguridad, específicamente en aquellos donde se operaba con sistemas basados en tecnología con banda magnética. En la búsqueda de una solución definitiva al problema, ASFI determinó la necesidad de que las Entidades de Intermediación Financiera (EIF) procedan a la migración al estándar EMV con tecnología chip. ¿Por qué se optó por el estándar EMV? La experiencia a nivel mundial ha demostrado que el estándar EMV es la tecnología más idónea para contrarrestar los fraudes informáticos. En América Latina, los bancos que implementaron esta tecnología mostraban una notable reducción en los niveles de fraude vinculados a las tarjetas de pago. Por ejemplo, con la implementación de esta tecnología Chile logró que el fraude en medios de pago se redujera sustancialmente hasta alcanzar un 0,025% en pérdidas sobre el total facturado, este porcentaje reflejaba el nivel

más bajo con relación a los países de toda Latinoamérica. En este contexto, el principal motivo para migrar al estándar EMV obedece primordialmente a razones de seguridad. Concordante con este criterio, un estudio reciente del Banco Central Europeo sobre esta temática señala que la mejora más importante fue la adopción más amplia del estándar EMV en la Zona Única de Pagos en Europa (SEPA). Es de resaltar que adicionalmente a las ventajas relacionadas con seguridad, la tecnología EMV permite a las entidades financieras generar nuevos servicios con valor agregado. Bolivia al adoptar el estándar EMV se suma a una corriente a nivel mundial que sigue la misma tendencia. Cifras reveladas por EMVco1 indican que alrededor de 1,2 billones de tarjetas EMV han sido emitidas globalmente y 18.7 millones de POS han sido actualizadas para aceptar tarjetas EMV. La tecnología EMV se está implementando exitosamente en más de 60 países a nivel mundial. Conceptualmente, el estándar EMV 2 se define como un estándar abierto que mejora la seguridad de la autenticación de la tarjeta contra la falsificación, verificación de titular contra pérdida o robo de tarjetas y la autorización de transacción contra la interceptación y reproducción. Este estándar afecta a los dos elementos de una transacción de pago con tarjeta, a la tarjeta que lleva incorporado el chip y el cajero automático o POS en el que se realiza la transacción (ambos deben estar adaptados para operar con esta tecnología). La incorporación del chip en la tarjeta de crédito o débito brinda mayor seguridad al momento de usarse porque la misma almacena la información de las operaciones realizadas en comercios a través de la compra de bienes y servicios o al operar en cajeros automáticos realizando operaciones de retiro de efectivo, consulta de saldos, transferencias de cuenta y servicios adicionales permitidos. La capacidad del chip de almacenar la información de las transacciones hace que sea muy difícil su clonación. En Bolivia, el proceso de migración del sistema financiero al estándar EMV ha sido planificado y supervisado por ASFI, sujeto a un cronograma de migración de tarjetas de crédito y débito, que fija las metas a ser cumplidas por las entidades de intermediación financiera. Entre las metas fijadas se destacan las

siguientes: a partir del primero de diciembre de 2012, los comercios comenzaron a aplicar los nuevos procesos de autorización de datos almacenados en el Chip en reemplazo de los datos de la banda magnética y desde esta misma fecha, los puntos de venta en comercios (POS) ya cuentan con tecnología EMV. Paralelamente, las EIF iniciaron el cambio de las tarjetas de crédito con banda magnética a tarjetas con chip. Para el 28 de febrero de 2013, se programó que las Tarjetas de Crédito con banda magnética deben ser reemplazadas en su totalidad por tarjetas con tecnología chip. Además, a partir del EMVCo es la organización creada en Febrero de 1999 por Europay International, MasterCard International, y Visa International para administrar, mantener, y mejorar las especificaciones para sistemas de pago con tarjetas con circuito integrado EMV (EMV Integrated Circuit Card Specifications for Payment Systems). 2 EMV, la tecnología que soporta a las tarjetas de crédito y débito, debe su sigla a la agrupación de empresas que la ha desarrollado e implementado: Europay, Mastercard y Visa. primero de marzo de 2013, los cajeros automáticos serán capaces de procesar transacciones en base a tecnología EMV y a partir de esta fecha ninguna tarjeta de débito será emitida sin contar con tecnología EMV. La finalización de todo el proceso de migración al estándar EMV en Bolivia concluirá el 31 de diciembre de 2013, cuando la totalidad de las tarjetas de débito sean reemplazadas con tarjetas con chip bajo el estándar EMV. A partir del primero de enero de 2014, todo el sistema de tarjetas de pago en Bolivia estará funcionando bajo el estándar EMV. La adopción de esta medida beneficia tanto a los usuarios financieros como a las EIF, obteniéndose en última instancia una reducción sustancial de los casos de fraude informático. Este factor es de suma importancia si se considera que los costes por fraude a nivel mundial se están incrementando (Nilson Report). En contraposición, la tendencia de los costos para adoptar el estándar EMV se han visto disminuidos, sobre todo si se comparan con los costos originales, incidiendo la demanda por esta tecnología que a nivel mundial se ha incrementado y permite a las empresas del ramo reducir sus economías de escala. El proceso de migración al estándar EMV no es

reciente, Europa inició el proceso hace aproximadamente 15 años. Sin embargo, el cambio de tecnología de banda al estándar EMV no es sencillo y representa un gran esfuerzo tanto para las entidades financieras como para la Autoridad de Supervisión, que vela por el cumplimiento del proceso, pero en última instancia, todo este esfuerzo está orientado a mejorar la calidad, la seguridad de las operaciones en resguardo de los ahorros de todos los usuarios financieros en Bolivia.