LA GESTIÓN DE RIESGOS OPERATIVOS EN LA SEGURIDAD FÍSICA EN EL SECTOR BANCARIO DEL PERÚ

JULIO BLADIMIR RIVERA VERA

COD. 2601030

JULIO CESAR GONZÁLES

ASESOR DE INVESTIGACIONES

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

DIRECCIÓN DE POSTGRADOS

ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTÁ

2016

Resumen

El riesgo ha estado presente en las diferentes épocas de la historia del hombre. Así hace 7500 años A.C. no existía la moneda y se corría el riesgo de trueques injustos, lo que para esa respuesta a ese riesgo se creó la moneda. En los 6000 años A.C. en Grecia, Egipto y en Mesopotamia no existía la contabilidad, por lo tanto, existía el riesgo en los negocios los cuales podían provocar pleitos y guerras, fue entonces que se empezó a medir los riesgos por medio de la contabilidad.

En la actualidad el riesgo en el ámbito empresarial nace con los problemas de errores intencionales y no intencionales, algunos convertidos en fraudes insalvables como los sucedidos a partir de 1998 con las grandes bancarrotas de empresas reconocidas de los EE.UU. y de Europa (WorldCom, Enron, Parmalat y muchas más).

Las organizaciones del ámbito empresarial requieren del manejo adecuado de las situaciones de riesgos que afectan su normal accionar. Entre algunas causales de riesgo encontramos los temas de seguridad física y material, aspectos que los clientes valoran como parte de la calidad del servicio que brinda la empresa. En este sentido, la gestión del riesgo está asociada a un proceso articulado y complejo cuya finalidad es reducir los riesgos sociales y las pérdidas económicas.

Asimismo, la gestión de riesgo implica establecer una infraestructura y estructura apropiada, así como desarrollar una cultura organizacional orientada a la prevención aplicando un método lógico y sistemático para lograr tener el riesgo bajo control. La gestión del riesgo es en sí misma, es un proceso que se inicia estableciendo el contexto operacional y luego identificando, analizando, evaluando y tratando los riesgos, mientras se supervisa y controla todo

el proceso y se comunica los resultados, minimizando las pérdidas económicas y aumentando los beneficios.

Para el caso del Sistema Financiero peruano, la Superintendencia de Banca y Seguros y AFP (SBS), ha definido parámetros que permiten a las empresas financieras supervisadas, implementar modelos de gestión integral de riesgos orientados a controlar a un nivel razonable los riesgos operacionales, monitorearlos y estar adecuadamente preparados para los cambios del negocio y el entorno, con una visión de las situaciones que pueden incrementar su exposición.

Los Bancos en el Perú utilizan el Método Básico para el cálculo de patrimonio efectivo por riesgo operacional, es por ello que surge la necesidad de analizar el proceso de gestión de riesgos operacional que viene aplicando para reducir las pérdidas económicas que se deriven de fallas en sus procesos, personal, tecnología o por eventos externos.

En dicho contexto, el presente ensayo busca específicamente analizar la Gestión de Riesgos en la Seguridad Física del Sistema Bancario del Perú; siendo este un tipo de riesgo recurrente en los bancos, y la reducción de pérdidas económicas derivadas del mismo.

Palabras clave: Skimming, Tarjeta con Chip o EMV, Banda Lectora, Sector Financiero, Perú.

Abstract

The risk has been present in the different periods of human history. 7500 years ago and B.C. there was the currency and the risk of unfair barters came, so for that response to that risk the currency was created. In the 6000 years B.C. in Greece, Egypt and Mesopotamia accounting did not exist, therefore, there was a risk in business, which could lead to lawsuits and wars, it was then that began to measure risks through accounting.

At present the risk in business is born with the problems of intentional and unintentional errors, some turned into insurmountable fraud as happened from 1998 with large bankruptcies of US companies recognized and Europe (WorldCom, Enron, Parmalat and many more).

From business organizations require appropriate management of risk situations that affect their normal action. Among some causal risk issues are physical and material security, issues that customers value as part of the quality of service offered by the company. In this regard, risk management is associated with an articulated and complex process aimed at reducing social risks and economic losses.

In addition, risk management involves establishing an infrastructure and appropriate structure and develop an organizational culture focused on prevention by applying a logical and systematic method for achieving keep under control the risk. Risk management is itself, it is a process that begins by setting the operational context and then identifying, analyzing, evaluating

and treating risks, while monitors and controls the entire process and the results are communicated, minimizing economic losses and increasing profits.

In the case of the Peruvian Financial System, the Superintendency of Banking and Insurance and AFP (SBS), has defined parameters that allow supervised financial companies, implementing models of integrated risk management aimed at controlling a reasonable level of operational risks, monitor them and be adequately prepared for business changes and the environment, with a view of situations that can increase your exposure.

Banks in Peru using the basic method for calculating regulatory capital for operational risk, which is why the need to analyze the process of managing operational risks being applied to reduce economic losses resulting from flaws in their arises processes, personnel, technology or external events.

In this context, this essay seeks to analyze specifically Risk Management in Banking System Physical Security of Peru; this being a type of recurrent risk in banks, and reducing economic losses arising therefrom.

Keywords: Skimming, EMV Chip Card, Reading Band, Financial Sector, Perú.

Introducción

El presente trabajo de grado pretende dar a conocer la problemática que se está presentando, día a día en aumento, del fraude en cajeros automáticos en el Sistema Financiero Peruano, mediante la clonación de tarjetas de débito y crédito; el análisis realizado comprende desde la implementación del primer cajero en la historia mundial hasta la influencia de los mal llamados delitos financieros y en las operaciones transaccionales de tarjetahabientes.

La Gestión del Riesgo Operativo en el Banco de la Nación se viene realizando desde el año 2004, a partir del compromiso de su Directorio para implantar en cada uno de los procesos del Banco, la Gestión Integral de los Riesgos. Si bien la Gestión de Riesgos Operacionales, debe ser realizada de acuerdo a lo establecido en el Manual de Gestión de Riesgos, actualizado a octubre del año 2010, si no se logra la participación activa de todo el personal del Banco en dicha gestión, ello podría implicar la materialización de riesgos y en consecuencia la generación de pérdidas económicas para el Banco.

En dicho contexto, los Bancos en el Perú presentan riesgos operativos asociados a la seguridad física en sus diferentes agencias a nivel nacional, los mismos que se derivarían de desperfectos y/o inoperatividad de alarmas, inadecuada infraestructura de sus oficinas, sumado a la reducida cantidad de efectivos policiales, etc.

Al respecto, las Divisiones de Riesgos Operativos de los Bancos, deberán actualizar el Manual de Gestión de Riesgo Operativo, a fin de asignar claramente las responsabilidades en la

implementación de planes de mitigación, los plazos de ejecución de los mismos, así como los procedimientos de seguimiento y monitoreo de la efectividad de los controles que se generen para para reducir el nivel de riesgo.

La seguridad, confianza y tranquilidad de la población usuaria de servicios financieros, son aspectos de vital importancia para las entidades bancarias, por lo cual estas deben contar con políticas adecuadas y procedimientos que les permitan identificar y gestionar los riesgos operativos que pudieran impactar negativamente en dichos aspectos perjudicando los intereses de sus clientes y por ende de la sociedad.

Rubio (2008) en el trabajo de investigación titulado “Propuesta Metodológica para la Gestión del Riesgo Operativo, en los Procesos de Afiliación y Cotizaciones del ISSFA (Instituto de Seguridad Social de Fuerzas Armadas)” tiene como objetivo general identificar los factores críticos de riesgo operacional en los procesos de Afiliación y Cotizaciones del Sistema de Seguridad Social Militar Ecuatoriano, con el fin de establecer una propuesta metodológica, que sirva de instrumento para el adecuado manejo del riesgo de operación en los mismos, de tal manera que se dé cumplimiento a lo establecido por la Superintendencia de Bancos y Seguros, y al mismo tiempo, se reduzcan las pérdidas que se derivarían de éste.

Este trabajo presenta como principal conclusión, que, el ISSFA a pesar de haber creado la Unidad de Riesgos, no ha dado la importancia y el apoyo correspondiente a la gestión del Riesgo operativo, al no dotarle del recurso humano y material capacitado, para esta función; sin embargo, el presente trabajo constituye una muestra del interés en los responsables de los

procesos claves de lograr establecer un esquema eficiente de administración del riesgo operacional.

A su vez, la Superintendencia de Banca y Seguros del Perú, señala en el Reglamento para la gestión del riesgo operacional (Resolución SBS N° 2116-2009) que las empresas de servicios complementarios y conexos señaladas en el artículo 17° de la Ley General se sujetarán, para la gestión de su riesgo operacional, a lo establecido en sus normas específicas. Asimismo, podrán tomar en consideración las disposiciones señaladas en el presente Reglamento en función a su tamaño y complejidad.

El presente Reglamento será de aplicación a las empresas señaladas en el artículo 16° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas. También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Por su parte, Fernández (2010), ha explorado la gestión de riesgo en su obra “La gestión del riesgo operacional: de la teoría a su aplicación” dónde señala que el sistema financiero español ha realizado grandes esfuerzos en la gestión del riesgo operacional y, en consecuencia, en poco tiempo se habían alcanzado importantes avances, pudiendo afirmar que en líneas

generales se encuentra al nivel de los principales sistemas financieros de otros países. Sin embargo, son evidentes las diferencias entre algunas entidades ya que mientras algunas habían percibido rápidamente las ventajas que esta gestión les iba a suponer, otras solo se movían impulsadas por los requerimientos legales y no le dedicaban toda la atención necesaria.

Aunque las exigencias de capital de Basilea habían sido un importante acicate, todas seguirían con sus procesos, aun en el caso de que Basilea se hubiese retractado, porque habían comprobado la necesidad de su gestión y las ventajas en cuanto a la creación de valor de las entidades.

Introducir de forma generalizada el riesgo operacional en la cultura de las organizaciones era el principal reto al que se enfrentaron las entidades. En 2004 todas las entidades encuestadas ya habían adoptado la definición propuesta por el Comité de Basilea, a pesar de que, aunque la clasificación de eventos y la división por líneas de negocio seguía planteándoles problemas a la hora de su implementación en la práctica.

Las pérdidas operacionales por “ejecución, entrega y gestión de procesos”, junto con los “fraudes externos e internos” eran las categorías más frecuentes y de mayor impacto para la mayoría de las encuestadas. Mientras que la “banca minorista”, “banca comercial” y “negociación y ventas” eran las tres líneas de negocio más afectadas por pérdidas operacionales.

Para Fernández, el estudio permite un acercamiento al riesgo operacional desde varios enfoques y busca sensibilizar a la comunidad financiera, profesional y académica en torno a este

riesgo, así como a una gestión más proactiva del mismo. El avance de la tecnología va muy de la mano con los diferentes métodos desarrollados para atentar contra el sector bancario, afectando principalmente a sus clientes, pero de igual manera, se han implementado métodos que contribuyen a brindar mayor seguridad en las transacciones realizadas.

A su vez se identificaron las principales recomendaciones de seguridad tanto en el momento de recibir las Tarjetas (el plástico), como en el que es utilizado en los cajeros automáticos, principalmente en gasolineras y restaurantes, sitios de mayor preferencia del actuar delincuencial, después de los propios cajeros automáticos.

El Sistema Financiero se ha preocupado por brindar confianza a sus clientes y ha creado con ayuda del poder Legislativo leyes para proteger el bolsillo de los peruanos y coadyuvar a la mitigación del riesgo al que se están expuestos día a día los tarjetahabientes (usuario de una tarjeta de crédito y débito). De igual manera, han creado mecanismos de solución rápida y certera al brindar soluciones en el menor tiempo posible a reclamaciones por transacciones no reconocidas, como, por ejemplo, el abono del dinero hurtado a través de retiros fraudulentos, creando así, aunque no del todo confianza y credibilidad en el sector.

EL FRAUDE EN CAJEROS AUTOMÁTICOS MEDIANTE CLONACIÓN DE TARJETAS DE DÉBITO Y CRÉDITO

El Origen de la palabra cajero proviene del griego autómatas, cuya definición es que funciona por sí solo, sin ayuda de nadie. El primer cajero automático en el mundo fue puesto en marcha en el año 1959 en la ciudad de OHIO, Estados Unidos creado por Luther George Simjain quien había nacido en Turquía.

En este año se conoció el primer cajero avalado por Corporación Citi (CITICORP), pero este no dio los resultados esperados, porque las personas usuarias de este, eran aquellas que sentían disgusto al ver a los empleados de los bancos pendientes en sus operaciones de manejo de dinero y por lo tanto, al corto tiempo fue cerrado.

En el año 1965 el señor John Shepher-Barron decidió desarrollar una máquina revolucionaria que le entregara dinero a las personas, y tomando como base las máquinas expendedoras de chocolates de la época, fue así como en el año 1967, este escoces logró instalar su modelo de cajero automático en el Centro Financiero en la sucursal del Banco Barclays, ubicado en la ciudad de Londres; su funcionamiento se basaba en insertar cheques radioactivos, seguido de una clave de 4 dígitos. Todo un éxito en ese momento.

Las redes financieras juegan un papel muy importante ya que día a día son más sofisticadas y contribuye al tráfico de efectivo inclusive en las economías más desarrolladas, la mayoría de cajeros van conectadas a las redes interbancarias que les permite a los cuentahabientes realizar

retiros y depósitos en bancos diferentes a donde tienen sus cuentas, las redes interbancarias más conocidas son New York Currency Exchange (NYCE), Cirrus, Plus, Interac, entre otras.

Actualmente se estima la existencia de 2.3 millones de cajeros automáticos en todo el mundo según The ATM Industry Association, donde los países con mayor número de cajeros automáticos instalados son: Estados Unidos, Canadá, Europa, Latinoamérica, Asia-Pacifico, Asia, África y Medio Oriente, y para Latinoamérica los países a la vanguardia en cajeros automáticos son: Argentina, Brasil, Chile, Perú, México y Venezuela, relación que va directamente proporcional al número de población de estos países por ser los más grandes de la región.

En el mercado mundial se conocen dos tipos de tarjetas: las Tarjetas de Débito, con la cual se puede llevar un mejor control de los gastos, debido al cargo directo por el valor del retiro en los cajeros automáticos y cuya utilización depende del saldo que posea el cuentahabiente en su cuenta corriente y/o ahorros, y las Tarjetas de Crédito son una forma de financiación directa porque permiten desembolsar dinero mediante avances en los cajeros automáticos y en las mismas oficinas bancarias mediante un cupo previamente autorizado por la entidad financiera donde el cuentahabiente se obliga a devolver este dinero mediante el pago de cuotas de capital más intereses previamente pactados con el banco emisor.

Niveles de seguridad en los cajeros automáticos

Estos deben ser lo más óptimos posibles tanto para la entidad bancaria como para el cuentahabiente ya que prestan un servicio permanente y continuo, por tanto, se hace necesario contar con medidas de seguridad físicas tendientes a minimizar los riesgos a los cuales se encuentran expuestos.

En el Sistema Financiero Peruano se han dado pautas de seguridad en las nuevas instalaciones de cajeros automáticos, según acuerdos interbancarios vigentes en donde se dictan recomendaciones en seguridad física a seguir, principalmente en lo concerniente a ventilación, tipo de pared o mampostería (muros a base de bloques), tipo de puerta a colocar y cerradura a utilizar en el espacio asignado al usuario, tipo de caja fuerte dentro del cajero automático, anclaje de la caja fuerte al piso, el tipo de cableado y accesorios de seguridad en general.

La integridad transaccional en los cajeros automáticos se fundamenta en la transmisión del total de la información en forma encriptada y segura, lamentablemente no siempre se considera integración con sistemas de confianza, los datos sensibles considerados como la información personal que son los requeridos legalmente para evitar el fraude es el Número de Identificación Personal (PIN) al cual únicamente el cuentahabiente debe tener acceso, esta información sensible está encriptada con algoritmos para cifrado y descifrado de datos que garantiza la no alteración de datos cuando viaja la información entre el cajero automático y la entidad bancaria autorizadora.

Para proteger la identidad de los clientes las compañías fabricantes mundiales de los cajeros automáticos, que no son muchos, han tomado medidas o mejoras en su construcción con el fin de salvaguardar a los cuentahabientes para que puedan realizar operaciones seguras, lejos de las amenazas externas por parte de los criminales quienes entre otras, unen teclados falsos a los verdaderos y/o colocan lectoras de bandas de tarjetas en las máquinas. En algunos países se han implementado sistemas de identificación de clientes como lectura de huellas, reconocimiento de venas de las manos y reconocimiento facial.

Figura 1. Cajeros Automáticos o ATM (Automated Teller Machine).

Fuente: Imágenes de la Unidad de la Policía Nacional del Perú de Seguridad Bancaria "Águila Negra".

La seguridad del cliente, para el sistema financiero nacional, es una de las principales prioridades actuales ya que busca brindar a los usuarios tranquilidad y seguridad en el momento

de realizar sus transacciones en los cajeros automáticos. Los esfuerzos están concentrados en la prevención de retiros forzosos, en la clonación de las bandas de las tarjetas y los hurtos del efectivo posteriores a la transacción. Se ha adoptado entre otras, un sistema de alarma silenciosa que consiste en digitar el PIN, por parte del usuario de forma inversa, el cual envía un aviso a la entidad bancaria sobre una amenaza en curso. También, por ejemplo, en algunas entidades financieras el cajero automático se encuentra dentro de un hall bancario, accesible las 24 horas del día, contando con una gran cobertura de cámaras de seguimiento, teléfono de cortesía con comunicación directa con el personal del Banco y vigilantes privados de seguridad. Adicionalmente, la mayoría de cajeros automáticos de última generación disponen de espejos ubicados encima de la espalda del usuario permitiendo observar cualquier tipo de movimiento anómalo y que pueda poner en peligro su transacción.

Actualmente la falsificación del papel moneda es una de las mayores preocupaciones del gobierno y del sector financiero, ya que ésta se produce sin la conformidad legal del Estado y se asemeja bastante a la moneda real, tan similar como para hacerse pasar por original. La falsificación del papel circulante afecta a extranjeros y a nacionales, disminuyendo la confianza en la legitimidad del mismo, conllevando a otros delitos como la estafa o el timo. La emisión del papel circulante debe estar en cabeza del organismo oficial, que para el Perú es el Banco Central de Reserva. Otro factor es el desconocimiento de la ciudadanía de las características del papel circulante que contribuye a consumar el ilícito, logrando buena rentabilidad sumado esto a una justicia muy débil la cual no castiga severa ni ejemplarmente, y que están tipificadas en la Ley 26714 del 26 de Diciembre de 1996.

La emisión total nacional de tarjetas de débito y crédito y que se encuentran en poder de los cuentahabientes del Sistema Financiero Peruano, tienen todavía la banda magnética de lectura las cuales siguen siendo vulnerables y se encuentran expuestas a copias de información. Se han detectado fuentes para el copiado de esta información personal en datafonos ubicados en los comercios y elementos skimning acompañados de micro cámaras dispuestas en los mismos cajeros electrónicos, permitiendo registrar las claves y robar así la información contenida en la banda de la tarjeta.

Figura 2. Elementos skimming.

Fuente: Imágenes Programa Integral de Seguridad Bancaria – PISB de ASBANC.

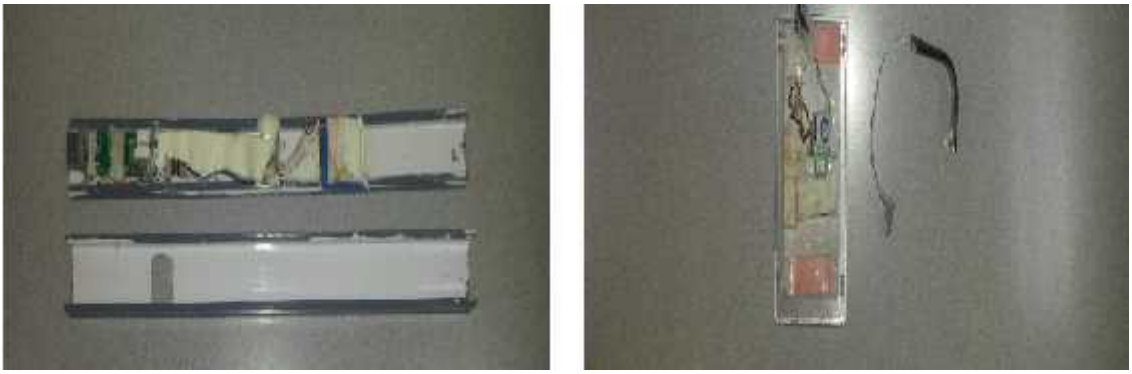

Figura 3. Elementos skimming.

Fuente: Imágenes Programa Integral de Seguridad Bancaria – PISB de ASBANC.

Preocupados por el alto índice de clonación, tres importantes compañías de reconocimiento mundial como son Europa, Master Card y Visa, desarrollaron tarjetas inteligentes dotadas de un chip, en donde se almacena toda la información del tarjetahabiente; cuando esta Tarjeta es introducido en el lector del cajero automático la bloquea y no permite su retiro, hasta cuando no se termine la transacción, garantizando así, confiabilidad y seguridad para el cuentahabiente tanto en tarjetas débito como crédito.

Recordando algo de historia se tienen Los Fraudes Financieros más famosos y que son recordados por su alto impacto social, tales como: Carlo Ponzi, italiano, estafador de los años 20 su negocio era una pirámide, consistía en pagar a los primeros inversionistas ganancias de las inversiones de clientes posteriores. Montó la empresa Securities Exchange Company prometiendo ganancias del 50% en tres meses. Fue condenado a 14 años de prisión.

Peter Young, gestor de fondos de los años 90, empleado del Banco Morgan Grenfell, tomaba el dinero que se encontraba en tres grandes fondos del Banco comprando acciones con alto nivel de riesgo y así obtenía grandes beneficios económicos. Las autoridades se dieron cuenta en un momento y detuvieron la comercialización de los mismos. Fue tal la presión hacia Young, que finalmente perdió la razón y fue internado en un Hospital Psiquiátrico.

Nick Leeson, Operador Británico de la Bolsa, quien ocasiono la quiebra del Banco Barings con 223 años de tradición. Sus acertadas inversiones le generaban al Banco grandes ganancias, pero abrió una cuenta secreta donde escondía parte de sus operaciones y así engañaba al Banco diciendo que invertía por otros cuando era dinero de la entidad. (Brújula Financiera. 2013)

Enron Corporation, Empresa Americana que vendía acciones, mediante la falsificación de documentos que aseguraban altas rentabilidades, cuando en realidad estaba en quiebra, costándole la vida y la reputación a los directivos de la compañía.

Bernard Madoff, Presidente de una firma de inversión muy importante en Wall Street. Detenido y sentenciado a 150 años de prisión por un fraude de 50 mil millones de dólares.

Delitos financieros en Perú

Nacieron a raíz de la emergencia económica, debido al mal comportamiento de algunos banqueros y de la captación ilegal de recursos del público en general, hechos que generaron pérdidas monetarias a los ciudadanos. La falsedad genérica se encuentra tipificada en el Art. 438 del Código Penal Peruano, que en señala:

La falsedad genérica se da simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde, suponiendo viva a una persona fallecida o que no ha existido o viceversa, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.

Uno de los delitos más reconocidos en los últimos tiempos en Perú, fue la Pirámide del Centro Latinoamericano de Asesoramiento Empresarial – CLAE. Esta institución fundada por Carlos Manrique Carreño logró mover cientos de millones de dólares sin rendir cuenta a nadie,

engañó a más de 200 mil personas de todos los estratos económicos y es considerada la estafa económica más grande que se perpetró en el Perú. En los años de brillo de CLAE, la empresa de Carlos Manrique ya no suscribía decenas de contratos por depósitos, sino miles hasta llegar a concentrar cientos de millones de dólares que representó en un momento el 40% de la liquidez del sistema financiero peruano.

Los delitos tipificados como suplantación de titulares, fraudes mediante cheques, retiros engañosos, copiado de información de las bandas magnéticas de tarjetas representan una preocupación bastante fuerte para el Sistema Financiero Peruano y de los mismos cuentahabientes, quienes finalmente son catalogados como los principales responsables directos de estas actividades y deben por ello iniciar una batalla para demostrar que no son transacciones autorizadas por ellos y reclamar la devolución de su dinero y el resarcimiento de su nombre ante entidades de control como centrales de riesgo.

El uso de medios tecnológicos como computadoras, escáner, software espías permiten a los delincuentes bancarios adulterar el Documentos Nacional de Identificación, pasaportes, títulos de vehículos, certificados laborales, poderes en general con tal éxito que pasan desapercibidos cumpliendo con los controles establecidos en el sistema financiero logrando así cumplir con su objetivo de timar.

Las estadísticas revelan, según KPMG Perú (firma miembro de Peat Marwick International -PMI y Klynveld Main Goerdeler -KMG), en su documento, denominado encuesta de fraude en Perú 2013, indica que el delito financiero, es el más sofisticado, su incidencia es del 10%, pero

su daño en las compañías puede llegar a ser del 51% en donde se afectan las oportunidades económicas de crecimiento, estancamiento de nuevas líneas de negocios, pérdida de empleos, este tipo de ilícito se conoce como el registro de ingresos para alterar cifras contables, registro de ventas ficticias, depreciar activos a mayor plazo al estimado, contabilizar arriendos de ciertos activos en lugar de manejarlo como arriendo financiero, según la experiencia del sector, la mayoría de la veces, este tipo de delitos, es cometido por altos cargos directivos, conocido como delito de cuello blanco; el 90% de fraude financiero es descubierto generalmente al año de haberse cometido y el 9% entre 5 y 10 días después de consumarse el delito, el 51% de estos delitos inician con la investigación generalmente por denuncia. Es importante resaltar que este tipo de delito representa el 1% del PIB Nacional. En la actualidad se hablan de tres métodos de delitos financieros como lo son el Pharming, el cual permite redireccionar un nombre de dominio, el Phishing enfocado en la suplantación de la identidad y el Malware, un programa cuyo objetivo es buscar entrar y dañar un computador, métodos que le han representado a los peruanos perdidas de U$ 40 millones, esto quiere decir que casi 10 millones de peruanos han presentado algún tipo de fraude en el sector.

Con el desarrollo de nuevos programas de software y elementos de hardware, los delitos financieros se han incrementado notablemente siendo recurrentes, ya que la suma de estas estructuras buscan infringir todo lo relacionado a nivel de tecnología como por ejemplo ingreso legal a programas, interceptación ilegal de redes, borrado, alteración o supresión de información, ataque a sistemas, muchas veces realizados por expertos hackers llegando a realizar el fraude electrónico en los sistemas de las entidades financieras. Los delitos financieros tienen como objetivo las redes de computadores para la instalación de software con archivos maliciosos

produciendo virus para espiar, obtener información clasificada de forma fraudulenta, conllevando a la sustracción de dinero, también mediante el uso del Pishing que es el uso de logos de entidades financieras mediante engaños busca que los tarjetahabientes envíen claves de acceso vía internet. Otro método usado es el Spam que son correos electrónicos no autorizados para propósitos no comerciales y finalmente está el uso de la ingeniería social la cual consiste principalmente en obtener información de personas sin su autorización aprovechando sentimientos como la curiosidad, avaricia, miedo y exceso de confianza, fenómeno ligado al crecimiento de las redes sociales, email y comunicaciones on line, anteriormente no era fácil engañar a los usuarios y los equipos de cómputo se bloqueaban o se ponían lentos, hoy en día es más difícil la detección porque el Malware ingresa al equipo y permanece estático y oculto hasta el momento propicio para poder atacar, es importante inculcar en la educación métodos de prevención para el robo de identidad.

El robo de la información de las tarjetas en el momento de cada transacción es utilizada para reproducirla, para su posterior uso fraudulento, estos hechos se presentan por lo general en restaurantes, gasolineras donde siempre hay un cómplice del establecimiento encargado del copiado de la información, en el caso de cajeros automáticos se coloca un dispositivo a través de la lectora de tarjetas la cual lee la información de la banda magnética, en combinación con micro cámaras las cuales graban el código pin del usuario, dificultando que el tarjetahabiente identifique el elemento Skimming, ya habiendo obtenido la información de la banda y el numero pin, esta se coloca sobre una tarjeta falsificada y proceden a realizar compras y retiros fraudulentos.

Figura 4. Modalidad de Robo de Información de Tarjetas de Crédito – "Skimming".

Fuente: Imágenes de la Unidad de la Policía Nacional del Perú "Águila Negra".

Confiabilidad en los cajeros automáticos

Es vital, de allí depende el éxito del uso de los mismos, cabe mencionar que todos los cajeros automáticos antes de ponerlos en funcionamiento han pasado numerosas pruebas que van desde la ubicación hasta la dispensación confiable de dinero y el funcionamiento correcto de la red, sin embargo se presentan casos como la dispersión de billetes falsos, o dinero entregado sin descontar de la cuenta del cliente o generan debito sin la entrega o dispensación del dinero, para asegurar la credibilidad en los cajeros automáticos estos cuentan con una revista rollo que es donde se almacenan todas las transacciones, éstos rollos van dentro del cajero y sirven de soporte en caso de una disputa entre el tarjetahabiente y la entidad bancaria.

Legislación vigente

Para contrarrestar los delitos financieros que atentan contra la población en general, el Estado Peruano ha creado una serie de leyes encaminadas a luchar contra el delito y salvaguardar la economía de los tarjetahabientes en contra de organizaciones delictivas dedicadas a este tipo de delitos y así disminuir este flagelo que tanto afecta a la sociedad. Entre las principales leyes tenemos:

Tabla 1. Protección de la información y de los datos - Ley 29733 de 2011.

Artículo 13	Alcances sobre el tratamiento de datos personales
Artículo 14.	Limitaciones al consentimiento para el tratamiento de datos personales
Artículo 17.	Confidencialidad de datos personales
Artículo 19	Derecho de acceso del titular de datos personales
Artículo 20	Derecho de actualización, inclusión, rectificación y supresión
Artículo 29.	Creación, modificación o cancelación de bancos de datos personales
Artículo 34.	Registro Nacional de Protección de Datos Personales
Séptima	Competencias del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi).

Fuente: Elaboración propia con datos de la Ley 29733 de 2011.

Habeas Data, Ley 26301 del 03 de Mayo de 1994, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia.

En el Código Penal Peruano, Art. 185 en los Delitos contra el Patrimonio, se encuentra consignado el Delito de Hurto, y en el Artículo 186 donde se tipifica los Delitos Informáticos, que consiste en el Hurto mediante la utilización de sistema de Transferencia Electrónica de Fondos, de la Telemática en general o violación del empleo de claves secretas.

Actualmente Perú cuenta con Entidades Asociadas encargadas de regular y controlar actividades del sector financiero y comercial. Estas entidades son:

Banco Central de Reserva del Perú (BCRP):

El Banco de Reserva del Perú fue creado mediante Ley Nro. 4500 del 09 de marzo de 1922, pero, es en setiembre de ese mismo año que se oficializa como BCRP, desde entonces, es considerado un organismo autónomo que tiene como finalidad preservar la estabilidad monetaria.

Para ello pone en marcha políticas que controlen la inflación, y en cierta medida, generen confianza en la moneda peruana, además, esto genera un estímulo al ahorro y a la inversión.

Podemos mencionar algunas de las principales funciones de esta institución:

Regular la moneda y el crédito.

Administrar las Reservas Internacionales.

Emitir billetes y monedas.

Informar sobre las finanzas nacionales.

Superintendencia de Banca, Seguros y AFP

Creada el 23 de mayo de 1931 como Superintendencia de Bancos, con la finalidad de controlar y supervisar a los bancos; en julio de 2000 se incorpora a su control y supervisión a las AFP, dejando el nombre de SBS, para tomar el actual: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

Es por ello, que esta institución está para proteger los intereses de los depositantes y asegurados preservando la solvencia de los sistemas supervisados (Bancos, Compañías de

Seguros, AFP'S); por lo cual, la Superintendencia abarca 02 grandes tareas primordiales: regular y supervisar.

Debemos informarnos antes de hacer algún tipo de movimiento bancario, puesto que no todas las instituciones brindan el mismo servicio, o el mismo goce de intereses; además cuando ésta infringe sobre los derechos del cliente, usted estará en todo el derecho de acudir a la institución pertinente para hacer los reclamos respectivos.

El aumento del riesgo en Perú, debido al crecimiento de ilícitos bancarios, ha ocasionado desconfianza en los cajeros automáticos, debido a los diferentes métodos implementados, cada vez son menos perceptibles para el cuentahabiente, generando malestar y prevención al uso de los mismos; sumado a esto la falta de entendimiento por parte de los bancos - clientes que deben iniciar investigaciones que a veces se llevan hasta meses sin dar una solución, ni respuesta efectiva, ocasionando un limbo del dinero no dispensado y siendo muy afectados. Es importante impulsar a las marcas y/o entidades dueñas del servicio de dispensación de dinero a desarrollar programas de fidelización donde no existan carencias, donde un cliente satisfecho trae otro comprador, mientras un cliente insatisfecho puede dañar la marca reputacional multiplicándose por las redes sociales, o el efectivo voz a voz, ocasionando una desconfianza total hacia el sector.

Las instituciones financieras en Perú como mecanismo alterno para brindar alguna solución efectiva a sus clientes después de haber interpuestos sus quejas y reclamos y luego de realizar una investigación exhaustiva tratando de brindar una solución favorable al tarjetahabiente, ofrecen seguros para cubrir reclamaciones por compras o retiros de cajeros automáticos no

realizados bajo su consentimiento, pólizas conocidas como Seguro de Fraude que inclusive incluyen robo de cheques, extravíos o hurto de tarjetas débitos o créditos y asaltos en cajeros automáticos y compras a través de internet.

El número de tarjetahabientes representan el segundo grupo más importante en montos después de la libranza (mecanismo de recaudo de cartera en donde el deudor autoriza a su entidad empleadora a descontar de su remuneración mensual o quincenal) y el primero en número de clientes y operaciones de consumo, al cierre del año 2012 se evidenció el uso del 36% del total del cupo utilizado sobre el aprobado, mientras que el 64% se mantiene muy pasivo y esto corresponde a tarjetahabientes con ingresos superiores que en algún momento de su historial crediticio han tenido una mala experiencia con el uso de la tarjeta.

El aumento desmedido del uso de mecanismos tecnológicos para realizar fraudes en los cajeros automáticos, el uso de Phishing (suplantación de identidad informática), de la inseguridad reinante ha traído como consecuencia la disminución de la transaccionalidad, aunque las entidades financieras buscan día a día dinamizar este uso con nuevas líneas de negocio no se ha logado convencer ni brindar el 100% de confianza al tarjetahabiente.

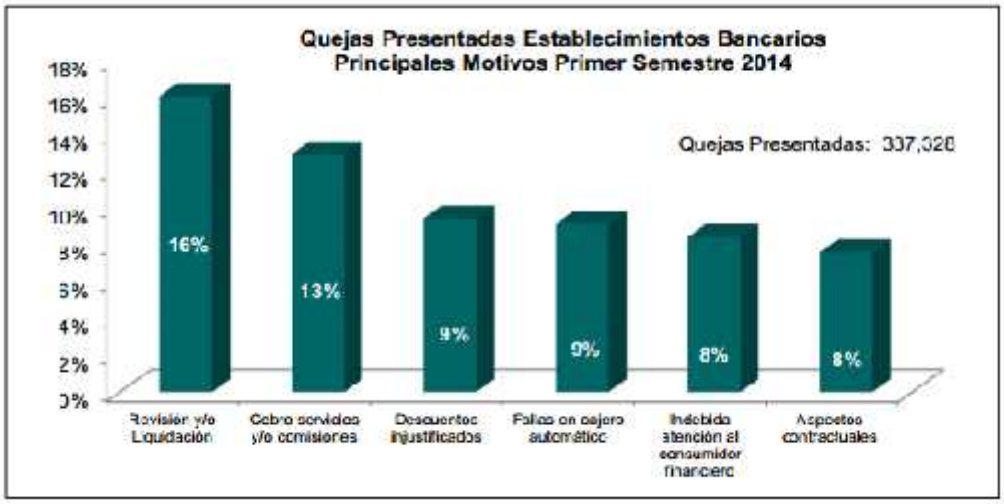

Figura 5. Quejas presentadas en el sector bancario durante primer trimestre del año 2014. Total Quejas 337828.

Fuente: Superintendencia de Banca y Seguros del Perú, (2014).

En la figura 3 se observa que las quejas con respecto a las fallas en los cajeros automáticos representan el 9% del total, equivalente a 30730 reclamaciones.

Las entidades financieras peruanas preocupadas por las operaciones fraudulentas con tarjetas débito y crédito, se han unido a la cruzada por la lucha contra este flagelo y han optado por medidas drásticas como, por ejemplo, la implementación de la tecnología EMV (Tarjetas con microprocesador – chips).

Vale la pena recordar que tanto las tarjetas de débito como de crédito cuentan con banda magnética que almacenan información en un revestimiento de óxido puesto en una tira plástica pegada a la tarjeta, esta tecnología es usada desde los años 70 y que aun sobrevive debido a facilidad de ser leídas por lectores especiales, pero con la desventaja hoy en día de ser copiada

con bastante facilidad la información allí almacenada y luego ser transferida a otra tarjeta o plástico para posteriormente ser utilizada en operaciones fraudulentas en cajeros automáticos y comercio en general.

Es por eso que debido a su larga duración en el mercado, los delincuentes han avanzado bastante en la clonación de las tarjetas, por su estancamiento en el uso de tecnología, así, preocupados por estas situaciones Europa, MasterCard y Visa unieron sus esfuerzos y decidieron cambiar el paradigma reinante por muchos años y crearon el modo chip inteligente o tecnología EMV en las tarjetas circulantes, cuyo principal objetivo es permitir la transaccionalidad a nivel mundial con mayor nivel de seguridad.

La tecnología aplicada en las tarjetas EMV es más difícil de ser copiada debido a los microprocesadores que poseen y su implementación debe darse a nivel mundial, en Perú, por ejemplo, se está utilizando con carácter obligatorio desde el año 2014, pero en Estados Unidos la regulación allí implementada la exige a partir de octubre del año 2015, lo que permite tener una brecha menor para la consumación de transacciones fraudulentas.

De igual manera, se han establecido una serie de recomendaciones muy válidas y poco utilizadas entre los clientes bancarios al momento de recibir las tarjetas, entre las más importantes, hay que destacar las siguientes: al momento de recibir las tarjetas asegurarse de que el sobre no haya sido abierto previamente, firmar la tarjeta una vez se ha recibido; evite perderla de vista al momento de realizar pagos; no prestar la tarjeta; memorizar el PIN, no lo escriba ni lo

guarde, este es personal e intransferible, la institución bancaria bajo ningún argumento le pedirá esta información mediante correos electrónicos o uso del teléfono.

En el uso delos cajeros automáticos las medidas de seguridad no se deben descuidar y se deben tener entra las más recordadas las siguientes: cubrir con las manos el teclado al momento de digitar la clave o PIN; no dar a conocer este número secreto; si en el momento de realizar la operación es abordado por un extraño con la intención de brindar ayuda, rechácela de inmediato; cuando termine la transacción en un cajero electrónico confirme la finalización de la transacción.

La suplantación de la identidad es usada de manera indiscriminada por la delincuencia para cometer sus delitos, a lo cual se recomienda: mantener los documentos personales en un lugar seguro y verificar constantemente su conservación allí; no facilitar la información personal mediante correos electrónicos y/o llamadas telefónicas; utilizar sistemas antivirus y un firewall personal (red diseñada para bloquear el acceso no autorizado y permitir al mismo tiempo comunicaciones autorizadas) en el computador personal y en del trabajo.

De todas maneras, si se ha sido víctima de robo en algunas de las modalidades mencionadas lo más convenientes es dar aviso a la autoridad competente, comunicarse con la entidad financiera donde se tenga la cuenta bancaria, colocar la denuncia respectiva y las alertas necesarias en las Centrales de Riesgo, como Data crédito, en la Policía Nacional del Perú y en el Programa Integral de Seguridad Bancaria de la Asociación de Bancos del Perú (ASBANC).

A pesar de las campañas a nivel nacional de autoridades, de entidades bancarias, de diferentes gremios, brindando permanentemente información a través de los diferentes medios de comunicación para contribuir a la disminución y erradicación de esta práctica, los tarjetahabientes se han visto expuesto a robos mediante fraudes en las tarjetas que poseen, incluyendo las de tecnología EMV, porque éstas, de todas maneras, cuentan con banda magnética, y aun así no están del todo blindadas.

El robo de tarjetas de débito y crédito en el territorio peruano es una práctica o evento que sucede todos los días y afecta a la mayoría de la población sin distingos de edad, sexo o clase social, el único requisito para estar expuesto a este flagelo es contar con una. Sin embargo, se pueden tomar algunas medidas preventivas que ayudan a mitigar esta práctica y sus efectos, una de las más importantes es tratarlas como si fueran efectivo constante y sonante, es decir, sin descuido.

Es así que bastantes establecimientos comerciales pasan la tarjeta con banda magnética en la terminal de compra y pueden copiar la información allí plasmada, en Perú, por ejemplo, la policía reportó un incremento del 25% en denuncias por clonación en el periodo comprendido del año 2012 al 2013.

El monitoreo transaccional es una de las herramientas 7x24 que han implementado las entidades bancarias para evitar y prevenir el fraude con tarjetas débito y crédito, este sistema funciona en línea y en tiempo real analizando y valorando la información proveniente de establecimientos comerciales, de cajeros automáticos y en fin de todo aquel sitio en donde se

puedan utilizar los plásticos en diferentes tipos de transacciones, conociendo de antemano de los tarjetahabientes sus rutinas de usos, de compras y retiros, información que es parametrizada en el sistema tecnológico de la entidad bancaria y ante un movimiento fuera de lo usual es confirmada directamente con el cliente.

Siendo conscientes del aumento a nivel nacional de los fraudes presentados con las tarjetas en todos los canales que se encuentran abiertos para la utilización de estas, se deben ampliar las medidas a tomar e implementar hacia los afectados tanto directos como indirectos y así, contribuir con la minimización del flagelo y de sus graves consecuencias a las que son expuestas las personas víctimas de esta situación, tanto a nivel económico, social y emocional.

Se debe entonces, mejorar en las prácticas y recomendaciones implementadas para evitar ser víctimas de este tipo de hurto, por lo tanto se propone reforzar la protección de identidades ligadas con las transacciones, así : utilizar una avanzada autenticación de clientes en los sistemas de información tecnológicos, asegurando la integridad en cada una de las transacciones; extender el uso de la firma digital mediante el uso de los Token cuya principal función es proteger a los clientes contra accesos no autorizados porque brindan claves dinámicas, verificar que no existan elementos extraños en las lectoras de tarjetas, en caso de la más mínima sospecha no utilizar el cajero, no usar cajeros automáticos en lugares apartados u oscuros, no utilizar claves sencillas relacionadas con fechas especiales o números telefónicos, no retirar grandes sumas de dinero, uso en el Internet: escribir siempre la dirección completa del sitio al cual se desea accesar, no seguir enlaces proporcionados por otras páginas de Internet, al renovar la tarjeta se debe destruir inmediatamente el anterior.

Así, por ejemplo, la clave del Token cambia automáticamente cada 60 segundos. En el extremo izquierdo de la pantalla se indica el tiempo que transcurrirá antes del próximo cambio, expresado en barras horizontales las cuales irán desapareciendo conforme se acerque el siguiente cambio de clave.

Figura 6: Token actual.

Fuente: Banco de la Nación - Perú, (2016).

El sistema financiero siempre ha estado expuesto a fraudes que han traído consecuencias de pérdidas monetarias, de imagen y de clientes. La confidencialidad en el manejo de este tipo de información sensible es básica para generar confianza hacia sus clientes, sin embargo, a diario se ven en los medios de comunicación noticias relacionadas y que van en detrimento del sector.

En la actualidad el sector bancario peruano es uno de los más importantes del sistema financiero, pues allí se concentran los depósitos y colocaciones internas en gran dimensión. Podemos decir entonces que, el riesgo operacional, que se genera en estas entidades, es

provocado por diversos factores y uno de ellos es por el incumplimiento normativo, específicamente por el incumplimiento de las medidas mínimas de seguridad (alarmas de agencia, la cantidad de efectivos policiales o vigilantes privados) que establece la SBS (Superintendencias de Banca, Seguro y AFP) lo que puede generar sanciones por parte de entidades reguladoras.

Figura 7. Procedimiento para la atención de Alarmas Bancarias.

Fuente: Imagen de la Unidad de la Policía Nacional del Perú “Águila Negra”.

Muchas veces se han perdido grandes cantidades de dinero por falta de seguridad en entidades financieras, si bien es cierto, la seguridad que brinda los Bancos es de empresas privadas, y el patrullaje motorizado, supervisión-control está a cargo de la Policía Nacional del

Perú por intermedio de la Unidad Especializada de Seguridad de Bancos “Águila Negra”, sin embargo, por no mitigar en el momento indicado dicho riesgo no solo se han generado pérdidas cuantiosas de dinero, sino lo que es peor, pérdidas humanas de clientes y trabajadores, es por ello que se debería de tomar gran importancia en gestionar este tipo de riesgos con un adecuado plan que permita tomar acciones inmediatas.

Otro punto en contra de la seguridad de las entidades bancarias, y al parecer los delincuentes y personas al margen de la ley, se han percatado es que el personal de seguridad (custodia armada) que resguarda los establecimientos bancarios no están debidamente entrenados y capacitados para enfrentar los planes ejecutados por organizaciones criminales. Según el congresista y ex ministro del Interior Octavio Salazar, el “profesionalismo” y la “nueva mira” de los delincuentes coinciden con una revelación del Departamento de Seguridad de Bancos “Águilas Negras”, que indica que casi el 95% de la seguridad de la entidades bancarias está a cargo de la Seguridad Privada, en vista de la disposición del gobierno central de que en los próximos meses la totalidad del personal policial deberá avocarse a la seguridad ciudadana y a dedicación exclusiva.

Conclusiones

A lo largo de la historia de los cajeros automáticos, se ha visto cómo han evolucionado en seguridad, en seguridad integral, tanto en elementos físicos como tecnológicos y de software, siempre tratando de brindar y ofrecer tranquilidad a los clientes, quienes al final de la cadena son los directos consumidores de este tipo de servicio.

Es así como amparados por lineamientos estándar a nivel nacional se han establecido en el sector financiero peruano una serie de recomendaciones al momento de las instalaciones de nuevas máquinas tratando de brindar seguridad en cada punto y así atraer más usuarios.

Muy a pesar de los grandes esfuerzos que se realizan día a día por parte de los involucrados como lo son los mismos fabricantes de los cajeros automáticos y el sistema financiero, la delincuencia cada vez ataca y perfecciona su delinquir en todas sus modalidades, como por ejemplo el robo de identidad para acceder a créditos bancarios, la suplantación, el robo de información en las tarjetas débito y crédito para retiro de dinero y compras a través de internet, de otro lado están el uso de software malicioso también siempre tratando de obtener información de los cuentahabientes para el usufructo delincuencial, también vale la pena mencionar los delitos llamados de cuello blanco realizado inclusive por los mismos directivos de las empresas o instituciones financieras.

La búsqueda continua de este objetivo es uno de los propósitos de cada uno de los actores intervinientes en esta cadena de servicios, en la que la meta es brindar al tarjetahabiente la

máxima seguridad en el momento de la transacción, tanto interna como externa, interna al brindar a los usuarios una transacción segura libre de toda duda por ejemplo en la originalidad del billete dispensado y externa , que esta sea segura en el momento de verdad de cada transacción, como por ejemplo que cada máquina se encuentre libre de elementos extraños de copiado de información.

Preocupado por este tipo de flagelo que afecta a todos los clientes y usuarios sin distinción de sexo, raza o clase social, el gobierno y la legislación peruana han dictado una serie de medidas que tienen como propósito disminuir este tipo de flagelo y mostrarle a la delincuencia que este tipo de delitos es castigado y que no es ignorado por el sistema actual, sin embargo a pesar de las disposiciones judiciales actuales vigentes y las condenas impuestas este aún no ha sido erradicado y se ve en tendencia creciente.

También con la implementación en el Perú desde el 2014 de nuevas tecnologías como la EMV se pretende erradicar en un futuro el nivel de transacciones fraudulentas, sobre todo con la ayuda de EEUU que a partir del 2015 tiene implementado esta tecnología en su sistema financiero.

De todas maneras, se está trabajando en forma conjunta a través del ASBANC y con diferentes gremios como el del comercio y el bancario realizando campañas de concientización dirigidas a los usuarios haciendo recomendaciones directas sobre el manejo y uso de sus tarjetas recordándoles en primera medida que estas no deben ser descuidadas ni perdidas de vista en

ningún momento y así evitar ser producto de la copia de información y posterior utilización fraudulenta.

La gestión de riesgos operativos en la seguridad física de las agencias bancarias está relacionada a la reducción de pérdidas económicas en los Bancos, los desperfectos en las alarmas de agencias, es uno de los riesgos más frecuentes que se presentan en torno a la seguridad física, son también los que podrían generar pérdidas económicas considerables para los Bancos al no tener existir una reacción inmediata de la Policía Nacional del Perú ante un ilícito penal que se presente en el interior de la agencia bancaria, en los cajeros automáticos y/o alrededores.

Se recomienda que las Entidades Bancarias del Perú, deben modificar sus respectivos Manual de Gestión de Riesgos Operativos, estableciendo claramente las responsabilidades específicas y los plazos de ejecución de cada etapa del proceso de Gestión de Riesgos Operacionales, incidiendo principalmente en la etapa de control - monitoreo (inspección a los sistemas de alarmas) y asegurar que el personal de seguridad asignado a las agencias, se encuentren adecuadamente capacitados para afrontar asertivamente hechos delictivos que se pudieran presentar; puesto que en la actualidad los Bancos han asignado a sus agencias, principalmente personal de seguridad privada los que en su mayoría no están capacitados y entrenados adecuadamente.

Referencias

Ayala, S, (2005) El sistema financiero.

Recuperado de: http://www.gestiopolis.com/canales5/fin/sistefinan.htm.

Asbanc. (2016). Conócenos.

Recuperado de: http://www.asbanc.com.pe.

Banco de la Nación (2010). Manual de Gestión del Riesgo Operacional.

Banco de la Nación, (2016). Token BN Perú.

Recuperado de: http://www.bn.com.pe/clientes/banca-internet/clave-dinamica.asp.

Brújula Financiera. (2013). Curiosidades. Los 5 fraudes financieros más famosos de la historia.

Carlo Ponzi, (19).

Código Penal Peruano, Delitos contra la Fe Pública - Art. 438 “Falsedad Genérica”.

Decreto Legislativo Nro. 635 del 03 de Abril de 1991. Código Penal Peruano.

Fernández L. A. (2010) Gestión del riesgo operacional: de la teoría a la práctica.

España: Fundación Uceif. Biblioteca Master de la Universidad de Cantabria.

Giménez-Montesinos, M. Á. N. (2005). El tratamiento del riesgo operacional en Basilea II. Revista Estabilidad financiera N.° 8. Banco de España.

KPMG. (2013). Encuesta de Fraude en el Perú 2013.

La Republica. (2012). 916 bancos de Lima son más vulnerables a los asaltos por ausencia policial.
Recuperado en: http://www.larepublica.pe/18-03-2012/916-bancos-de-lima-son-mas-vulnerables-los-asaltos-por-ausencia-policial.

Ley Nro. 4500 del 09 de Marzo de 1922. Ley de creación del Banco Central de Reserva del Perú.

Ley Nro. 26301 del 03 de Mayo de 1994. Ley de Habeas Data.

Ley Nro. 26714 del 26 de Diciembre de 1996. Ley de Falsificación de Billetes o Monedas.

Ley Nro. 29733 del 03 de Julio del 2011. Ley de Protección de Datos Personales.

Rubio P, A. (2008). Propuesta metodológica para la gestión del riesgo operativo, en los procesos de afiliación y cotizaciones del ISSFA. Tesis. Universidad Andina Simón Bolívar, Ecuador.

Superintendencia de Banca y Seguros y AFP. (2009). Resolución Nro.2116-2009 del 02 de Abril del 2009.