UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS VULNERABILIDADES, AMENAZAS Y RIESGOS DE LA PLATAFORMA WEB DE LA BANCA VIRTUAL DEL BANCO PICHINCHA

SISALIMA PINDO LEIDY MARCELA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÁLISIS DE LAS VULNERABILIDADES, AMENAZAS Y RIESGOS DE LA PLATAFORMA WEB DE LA BANCA VIRTUAL DEL BANCO PICHINCHA

SISALIMA PINDO LEIDY MARCELA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÁLISIS DE LAS VULNERABILIDADES, AMENAZAS Y RIESGOS DE LA PLATAFORMA WEB DE LA BANCA VIRTUAL DEL BANCO PICHINCHA

SISALIMA PINDO LEIDY MARCELA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 18 DE JULIO DE 2018

MACHALA
18 de julio de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Análisis de las vulnerabilidades, amenazas y riesgos de la plataforma web de la Banca Virtual del Banco Pichincha, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 3

Fecha de impresión: miércoles 18 de julio de 2018 - 13:49

Urkund Analysis Result

Analysed Document:	SISALIMA PINDO LEIDY MARCELA_PT-010518.docx (D40289066)
Submitted:	6/21/2018 6:47:00 AM
Submitted By:	lsisalima_est@utmachala.edu.ec
Significance:	3 %

Sources included in the report:

https://www.slideshare.net/gelysb/valoracin-de-banco-pichincha-portoviejo
http://www.seps.gob.ec/documents/20181/25522/Seguridad%20en%20Canales%20Electronicos.xlsx/b706ead4-c19a-441d-b8bf-f9ee07839b08

Instances where selected sources appear:

5

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, SISALIMA PINDO LEIDY MARCELA, en calidad de autora del siguiente trabajo escrito titulado Análisis de las vulnerabilidades, amenazas y riesgos de la plataforma web de la Banca Virtual del Banco Pichincha, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

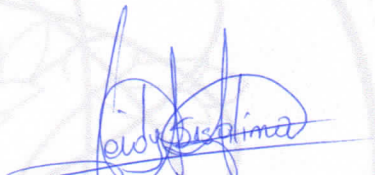
La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 18 de julio de 2018



SISALIMA PINDO LEIDY MARCELA
0705541647

RESUMEN

La presente investigación se refiere al Control Informático en los entornos virtuales de las entidades financieras, por lo que se hace indispensable identificar las vulnerabilidades, amenazas y riesgos que llegan a presentar las instituciones bancarias. Este es un proceso llevado a cabo por profesionales que se encuentran capacitados para este hecho y el cual consiste en un examen que tiene el carácter de objetivo, crítico, sistemático y selectivo con el propósito de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos de los que dispone la organización y si ésta se ha encargado de brindar los soportes necesarios para cumplir sus objetivos y metas. El objetivo del presente trabajo es: Identificar las amenazas, vulnerabilidades y riesgos de la Banca Virtual del Banco del Pichincha para contribuir a un mayor control y preservar la información.

Palabras clave: amenazas, vulnerabilidades, riegos, banca virtual, control

ABSTRACT

The present investigation refers to the Computer Control in the virtual environments of the financial entities, so it is essential to identify the vulnerabilities, threats and risks that come to present the banking institutions. This is a process carried out by professionals who are trained for this fact and which consists of an examination that has the character of objective, critical, systematic and selective in order to evaluate the effectiveness and efficiency of the appropriate use of resources information available to the organization and if it has been responsible for providing the necessary supports to meet its objectives and goals. The objective of this paper is to: Identify the threats, vulnerabilities and risks of Banco del Pichincha's Virtual Banking to contribute to greater control and preserve information.

Keywords: threats, vulnerabilities, risks, virtual banking, control

ÍNDICE

INTRODUCCIÓN

La innovación tecnológica y su uso dentro de la actividad bancaria, ha contribuido para que las instituciones financieras sean más dependientes de la tecnología y además de exponerse a grandes pérdidas y daño en su reputación ante posibles fallos o violaciones a su sistema. Por lo general esta amenaza se presenta ante la deficiencia en la integridad y confiabilidad del sistema; por lo tanto los aspectos relacionados con la seguridad de la información son de gran relevancia.

La presente investigación se refiere a la Auditoría informática en los entornos virtuales de las entidades financieras, por lo que se hace indispensable identificar las vulnerabilidades, amenazas y riesgos que llegan a presentar las instituciones bancarias. Este es un proceso llevado a cabo por profesionales que se encuentran capacitados para este hecho y el cual consiste en un examen que tiene el carácter de objetivo, crítico, sistemático y selectivo con el propósito de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos de los que dispone la organización y si ésta se ha encargado de brindar los soportes necesarios para cumplir sus objetivos y metas.

Es importante recordar que todas las empresas a nivel mundial se encuentran expuestas a nuevas amenazas que ponen en riesgo los sistemas informáticos y tecnológicos, situación que no es diferente en el Ecuador, donde la banca electrónica ha tenido un importante crecimiento, este tipo de problemas se encuentran con mucha frecuencia debido a que muchas de las organizaciones no se encuentran capacitadas para enfrentarlos por lo que se hace necesario, además de un buen control interno, la aplicación de prácticas efectivas que además se encuentren en consecuencia con lo que disponga la Ley.

El objetivo del presente trabajo es: Identificar las amenazas, vulnerabilidades y riesgos de la Banca Virtual del Banco del Pichincha para contribuir a un mayor control y preservar la información. Para dar respuesta al objetivo inicialmente planteado y

complementar la información se diseñan dos objetivos específicos: 1) Describir la importancia de la Auditoría Informática para prevenir las vulnerabilidades que puede presentar el sistema; 2) Proponer recomendaciones que contribuyan a prevenir este tipo de vulnerabilidades.

FUNDAMENTACIÓN TEÓRICA

Análisis preliminar

En el desarrollo de la innovación financiera, de las últimas décadas, en conjunto con los avances de las tecnologías de la información y la comunicación ha contribuido al incremento de la eficiencia en el sistema financiero y uno de los factores que han aportado a este crecimiento es el haberse trasladado hacia los medios electrónicos (Galán & Venegas, 2016). De acuerdo a (Layva, Alarcón, & Ortegón, 2016), la banca virtual es aquella donde son realizadas transacciones a través de internet, entre las características que presenta se encuentra la oportunidad de ahorrar tiempo, dinero y trámites al momento de realizar cualquier tipo de transacción financiera.

Si bien la banca electrónica ya no solo se encuentra asociada a los tradicionales canales electrónicos como la computadora y el internet, sino que en la actualidad se ha trasladado a los dispositivos móviles, por lo que dentro de este grupo, muchos autores también incluyen a la banca móvil (Borraz, Bordonaba, & Polo, 2016). Entre los productos ofrecidos a partir de las plataformas virtuales, se encuentran los siguientes: consulta de saldos, consulta de movimientos financieros, consulta de documentos, consulta de cheques, estados de cuenta, transferencias (directas y otras instituciones financieras), pago a proveedores, pago de remuneraciones, pagos de servicios, transferencias al exterior, entre otros.

El servicio virtual de los entidades bancarias busca ofrecer seguridad a las transacciones realizadas por sus clientes, de esta manera, luego de ser identificados por artefactos que previamente homologados, pueden interactuar directamente desde sus cuentas desde cualquier lugar y a cualquier hora, para lo cual se encuentra a disposición la red internacional de datos, la red de cajeros automáticos, el servicio de telefonía pública y para el desarrollo de esta actividad no requirió la intervención de ningún funcionario.

Riesgos, amenazas y vulnerabilidades de la Banca Virtual

Los riesgos, vulnerabilidades y amenazas a las que se enfrentan los bancos que se dedican a la electrónica, pueden ser agrupadas de acuerdo a las categorías de riesgo del Comité de Basilea, Este comité se encarga de la supervisión, a las entidades bancarias que operan a nivel internacional (López, 2013), en un informe se exponen ejemplos de riesgos específicos y problemas de los bancos que se relacionan con la banca electrónica y actividades de dinero electrónico, estos son: el riesgo operativo, el riesgo a la reputación y el riesgo legal.

Riesgo operativo.- Se relaciona con deficiencias importantes en la confiabilidad e integridad del sistema, con especial atención en los sistemas de seguridad debido a los ataques externos e internos. Para (Cruz & Alarcón, 2017) el riesgo operacional es dinámico y en la misma medida resulta cambiante y complejo tal y como se configura el entorno de las entidades bancarias.

Riesgo a la reputación.- Este se refiere al concepto que puede tener la sociedad de la institución financiera. De esta manera, aquellas condiciones que acrediten el respaldo social y el buen nombre de la organización en fundamental en la prestación de los servicios y genera confianza. Dentro de un sitio en internet, la seguridad estructural transmite la creencia de que el sitio presenta estructuras como contratos, garantías, protecciones legales y tecnológicas mejores (Muñoz, Sánchez, & Luque, 2014).

Riesgo legal.- Este surge a partir de las violaciones e incumplimientos de las leyes, reglas, reglamentos o prácticas que fueron establecidas, o también puede producirse cuando los derechos y obligaciones legales de las partes no se encuentran correctamente definidas. Entre los principales riesgos a los que se enfrentan se relacionan con la divulgación de los datos de los clientes y la protección a la confiabilidad.

Los usuarios de la banca electrónica se encuentran expuestos a vulnerabilidades, por lo que es necesario que las instituciones financieras consideren aspectos importantes en el diseño de un sistema bancario electrónico seguro. De acuerdo a un estudio realizado por

la Federación Latinoamericana de Bancos (Feleban), el 98,5% de los riesgos que presenta el sistema financiero son digitales e informáticos.

La vulnerabilidad es un fallo de seguridad, es decir es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente para lo que fueron diseñados, afectando la seguridad de los mismos, pudiendo en ocasiones provocar cosas como la pérdida y robo de información altamente sensible. Para (Crespo & Ramos, 2014), a la vulnerabilidad se la puede definir como la posibilidad de que una amenaza se materialice sobre un activo, incluyendo tanto elementos físicos como abstractos, es decir, información, servicios, etc.

La banca virtual en el Ecuador

En el Ecuador, el cliente de las instituciones bancarias dispone de cada vez un mayor número de servicios digitales, de esta manera, de los 23 servicios más comunes que se ofrecen en las entidades bancarias del Ecuador, al menos 16 ya se encuentran disponibles para ser realizadas en línea. Entre las innovaciones en las plataformas virtuales de los bancos se encuentra la apertura de cuentas por medio de aplicaciones móviles, hasta la obtención de documentos bancarios, como las referencias bancarias, desde la página web de la institución bancaria (González, 2017). Mientras que entre las transacciones más realizadas se encuentran el revisar el balance de las cuentas o comprobar las transacciones realizadas.

Pero a pesar de los buenos pronósticos que se manejan, aún se estima que el sistema bancario electrónico del Ecuador resulta insuficiente, donde aspectos como la falta de capacitación a los usuarios en cuanto al uso de los diferentes servicios, son evidencia del vacío existente en el sector.

Control Informático

En el actual escenario, donde las organizaciones realizan sus actividades dentro de un marco económico que se encuentra caracterizado por la globalización y por la interacción a nivel internacional de los mercados, donde por lo general se desarrollan dentro de un ambiente donde prevalece la competencia, como resultados de los

profundos cambios, se hacen necesarios el desarrollo de métodos e instrumentos que permitan establecer y además mejorar la forma en que actúan las organizaciones.

De esta manera, en todas las organizaciones, el manejo de la información debe ser gestionado bajos los mismos conceptos de eficiencia, eficacia y rentabilidad como con el resto de los activos organizativos. Si una organización desea mantenerse en el mercado y ser competitiva en el tiempo, es necesario que sean identificar, crear, almacenar, transmitir y utilizar de la mejor forma el conocimiento (Stable, 2012).

De acuerdo a Chamorro y Pino (2013), la gran complejidad de las medidas que se requieren para asegurar a los sistemas de información se hace más necesaria cada día, por lo que todas las personas que se muestran interesadas en el desarrollo de esquemas que contribuyan al cuidado de la información, a la actualización por el carácter globalizado de las tecnologías de la información, por la conectividad y la disponibilidad de esta, previniendo los delitos informáticos que son más frecuentes cada día.

En los últimos años, el uso de la informática se ha extendido hacia casi todas las actividades donde las redes de comunicación y por ende los sistemas de información han llegado a convertirse en algo de esencial valor para el desarrollo económico y social a nivel mundial. Siendo así que el garantizar la seguridad de la información ha llegado a ser una tarea de gran relevancia y preocupación para las organizaciones, ya sean estas del ámbito privado como en el público (Gil & Gil, 2017). Cuyo control se lleva a cabo Se lleva a cabo sobre estándares que son internacionalmente aceptados y de modelos de referencia que hacen especial énfasis en la mejor forma de que pueda ser gestionado (Hernández, 2010).

Proceso para determinar los riesgos, amenazas y vulnerabilidades de la Banca Virtual del Banco Pichincha.

El Banco Pichincha tuvo sus inicios en el Ecuador el 11 de abril de 1906, en ese entonces se constituyó como un banco de emisión, circulación y descuento, donde la entidad fijó desde sus inicios su prioridad que es la de trabajar en el mercado de divisas. En la actualidad es uno de los bancos con mayor consolidación en el Ecuador,

trasladándose también a las plataformas virtuales, donde los clientes realizan transacciones bancarias desde el computador. De acuerdo a la página web del banco, entre los beneficios de realizar transacciones en línea se encuentran las siguientes: ahorrar tiempo, acceder con facilidad a la información de la cuenta bancaria y realizar diversos tipos de transferencias.

Entre las principales transacciones que se pueden realizar desde plataforma virtual de la banca se encuentran: consulta de saldos y movimientos bancarios; transferencias directas e interbancarias; pago de servicios y tarjetas de crédito; referencias bancarias; recargas a diferentes servicios pre pago; inversiones; bloqueo de tarjetas; documentos electrónicos; otros servicios

Metodología

La metodología aplicada en el presente trabajo de investigación es de tipo descriptivo, de esta manera se podrá definir, clasificar, catalogar y de caracterizar el objeto de estudio. Se realiza a partir de la descripción de los hechos y fenómenos que se dan en la actualidad. Los métodos de investigación empleados serán una encuesta dirigida a los usuarios de los servicios virtuales del Banco Pichincha además de la observación. También se llevará a cabo una investigación de tipo documental, donde se recabará información de libros, revistas, publicaciones científicas, entre otros.

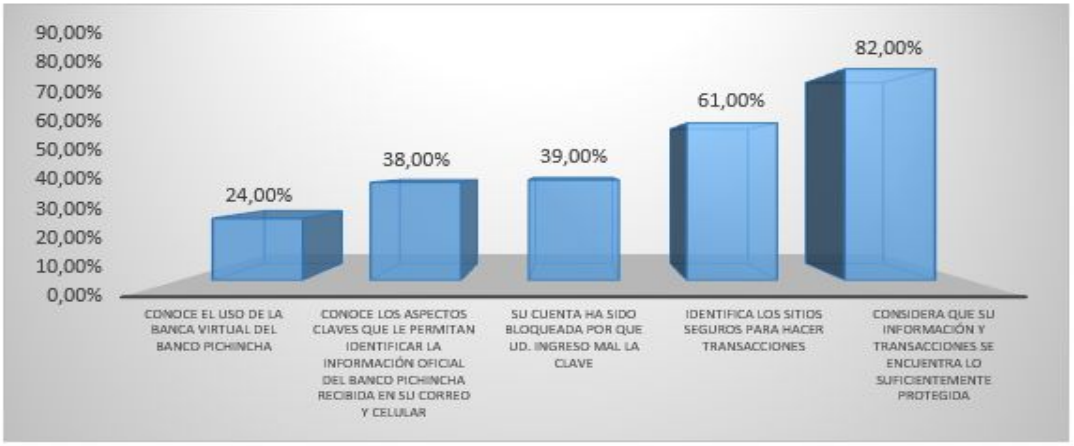
Control informático del Banca Virtual del Banco Pichincha

En base a lo enunciado, en el presente trabajo se analizará las amenazas, vulnerabilidades y riesgos de la Banca Virtual del Banco Pichincha, esta entidad bancaria, con el propósito de ofrecer mayor seguridad a sus clientes, pone en práctica varios mecanismos los mismos que van desde el envío de códigos de seguridad a los correos electrónicos de sus clientes hasta mensajes de texto a celulares que comunican sobre compras en línea o de transferencias bancarias. También ofrece servicios en cuanto al pago de servicios básicos como luz, agua, teléfono y televisión por suscripción. En las operaciones en línea también pueden ser cancelados los tributos, pagos a la Seguridad Social, pensiones de escuelas, colegios, entre otros.

El análisis de la seguridad informática de la Banca Virtual del Banco Pichincha se realizará a partir de una matriz riesgos. Los riesgos se identificaron de acuerdo a lo expuesto en los documentos consultados, donde se pone de manifiesto que en la actualidad el Banco Pichincha se encuentra entre las principales instituciones bancarias que hace uso de grandes innovaciones en seguridad informática, especialmente toman la información necesaria para actualizar sus sistemas en base a auditorías realizadas por compañías extranjeras.

Estas simulan un ataque virtual con el objetivo de verificar las seguridades del banco, de esta manera se identifican las fallas y se aplican los correctivos. Si bien la información de sus clientes se encuentra en datos encriptados y protegidos para evitar la sustracción de la información, no sucede lo mismo con los datos manejados por los propios clientes, donde por lo general la sustracción de la información se debe al mal uso que el cliente le da a esta (Baquerizo & Huilcapi, 2014). Para identificar los riesgos provenientes del uso del sistema al que tiene acceso el usuario se realizó una encuesta a las personas que acceden a la plataforma virtual (Anexo 1), de donde se obtuvo la siguiente información:

Figura 1 Encuesta control informático Banca Virtual.



Fuente: (Coronel, 2014)

Como se observa en la figura, el 24% de las personas encuestadas conoce el uso de la banca virtual del Banco Pichincha; el 38% identifica la página oficial de otras que posiblemente intente sustraer su información; en el 39% reconoce que su acceso a la cuenta fue bloqueado por un mal uso de la clave electrónica, el 61% menciona que

puede identificar los sitios seguros para hacer transacciones como compras en línea; el 82% indica que consideran que su información se encuentra bien protegida por las seguridades que ofrece la institución bancaria.

Con la información obtenida en la encuesta, adicional de la investigación documental realizada se realizas la matriz de riesgos es una herramienta de gestión que permite determinar de manera objetiva los riesgos que resultan relevantes para la seguridad, en este caso, de la seguridad informática que presenta la entidad bancaria.

Tabla 1. Matriz de riesgos Banca Virtual Banco Pichincha

N°	Factores de Vulnerabilidad, Amenazas y Riesgos	Impacto			Probabilidad			Nivel de riesgo	Recomendaciones
		A	M	B	A	M	B		
1	Desconocimiento del uso de la plataforma por parte del usuario	x				x		Alto	Informar y capacitar de forma permanente a los clientes, sobre los riesgos derivados del uso de los canales electrónicos y sobre las medidas de seguridad a considerar.
2	Medidas de seguridad para las transacciones realizadas.		x			x		Medio	Se debe disponer de controles de acceso adecuados al sistema bancario.
3	Verificación de identidad del usuario de la banca	x				x		Alto	Realizar pruebas de vulnerabilidad y penetración al sistema, si se diera el caso de que se realicen cambios en la plataforma que afecten a la seguridad de este canal, es indispensable realizar pruebas adicionales.
4	Bloqueo de cuenta y finalización de sesión		x				x	Medio	Informar y capacitar de forma permanente a los clientes, sobre los riesgos derivados del uso de los canales electrónicos y sobre las medidas de seguridad a considerar.
5	Reconocimiento de la identidad del sitio web	x				x		Alto	Informar y capacitar de forma permanente a los clientes, sobre los riesgos derivados del uso de los canales electrónicos y sobre las medidas de seguridad a considerar.

Fuente: La autora

Como se observa en la matriz de vulnerabilidades, riesgos y amenazas de la plataforma de la Banca Virtual del Banco Pichincha, el riesgo que se presenta es para el usuario debido a que las situaciones manifestadas ocurren por el mal uso de la plataforma o realizar procedimientos erróneos. De esta manera puede desconocer el correcto funcionamiento de la plataforma y cometer errores que terminen afectando el sigilo de su información, otro aspecto importante de resaltar es el de mayores controles en caso de un mal uso de la plataforma.

Con respecto a la verificación del usuario, este por lo general no se encuentra familiarizado con los métodos (mensajes de texto, reconocimiento facial, mensajes de correo electrónico) que puede ocasionar dificultad en el uso y por lo tanto vulnerabilidad para el aprovechamiento de terceras personas.

Aunque el banco tiene por seguridad la previsión de cerrar la cuenta unos minutos después de no realizar actividad alguna, muchos usuarios abren sus portales bancarios en equipos poco seguros que pueden terminar perjudicando los saldos bancarios del usuario. Y otro aspecto de gran importancia es el uso de páginas similares a la plataforma bancaria con el objetivo de robar las claves y ocasionar perjuicio al usuario. Todos los aspectos arriba mencionados se relacionan con la poca o casi nula capacitación que ofrece el banco a sus usuarios.

De esta manera la matriz de riesgos es de gran utilidad debido a que permite el análisis de los diferentes niveles de riesgos en las diversas áreas, a partir de la cual se proponen acciones concretas para disminuir los riesgos y además determinar el impacto que dichas acciones tienen sobre las actividades de la organización. De acuerdo a las vulnerabilidades, riesgos y amenazas identificados en la Banca Virtual, y con el propósito de garantizar la seguridad de las transacciones realizadas a través de la banca electrónica, las instituciones financieras que ofrezcan los servicios virtuales deben tomar en cuenta las siguientes consideraciones:

- **Riesgo: Desconocimiento del uso de la plataforma por parte del usuario,** los datos de índole personal y financiera deben encontrarse almacenados de forma segura y cualquier comunicación con el sistema de Banca en Línea debe encontrarse encriptadas, de esta manera se asegura la confidencialidad de los datos, los mismos que circulan desde los sistemas del banco hasta el navegador del usuario.

- **Riesgo: Medidas de seguridad para las transacciones realizadas.,** las páginas web de las entidades bancarias deben hacer uso de certificados de validez extendida, de esta manera se puede comprobar la identidad de los visitantes.

Estas certificaciones necesitan de verificaciones exhaustivas, además de otorgar un alto nivel de confianza.

- **Riesgo: Verificación de identidad del usuario de la banca,** con el propósito de obtener el más alto nivel de seguridad, el sistema de Banca Virtual, debe requerir de los más altos niveles de autentificación para acceder a la cuentas.

- **Riesgo: Bloqueo de cuenta y finalización de sesión,** para evitar la sustracción de la información, la cuenta debe ser bloqueada si la contraseña es introducida erróneamente. La sesión bancaria en línea será desconectada una vez que hubiesen transcurridos doce minutos de inactividad.

- **Riesgo: Identidad del Sitio Web,** muchas veces los usuarios reciben correos electrónicos, los cuales en apariencia son enviados por la institución financiera, donde se solicita el seguimiento a ciertos enlaces con el propósito de sustraerse información, ante lo cual resulta importante que las entidades financiera emprendan campañas para que los usuarios conozcan de estos posibles fraudes.

CONCLUSIONES

1. De acuerdo a los resultados de las encuestas realizadas y a la matriz de riesgo, la vulnerabilidad con mayor presencia se da por parte del usuario, cuando no sabe manejar la plataforma virtual de forma adecuada lo que puede ocasionar graves problemas como la sustracción de su información y perjuicio económico.

2. Por el lado de las instituciones bancarias, teóricamente se demostró que estas encuentran preparadas para enfrentar las vulnerabilidades en sus sistemas, pero en gran medida falta educar a los usuarios. Si los usuarios de la banca virtual pueden identificar a los peligros a los que se exponen, hay menos posibilidad de ser víctimas de robo. El Banco Pichincha es una de las Instituciones financieras que ha implementado modernos sistemas de seguridad con el propósito de resguardar la información de sus clientes.

BIBLIOGRAFÍA

Baquerizo, D., & Huilcapi, T. (2014). *Sistema Biométrico. Banco Pichincha.* Guayaquil: Universidad EcoMundo.

Borraz, J., Bordonaba, V., & Polo, Y. (2016). El cliente omnicanal en banca electrónica: un análisis del mercado español. *Tribuna de Economía*(891), 181-197. Obtenido de http://www.revistasice.com/CachePDF/ICE_891_181-198__865CDCD85868CB6FCC4C8E35BE83EC63.pdf

Chamorro, J., & Pino, F. (2013). *Modelo para la evaluación en seguridad informática a productos software, basado en el estándar.* Colombia: Universidad ICESI.

Coronel, K. (2014). *Auditoría Informática orientada a los procesos críticos de crédito generados en la Cooperativa de Ahorro y Crédito Fortuna, aplicando el marco de trabajo COBIT.* Loja: Universidad Técnica Particular de Loja.

Crespo, M., & Ramos, R. (2014). *Estudio del impacto financiero de las vulnerabilidades de las páginas web de los bancos en el Ecuador.* Guayaquil: Universidad Politécnica Salesiana.

Cruz, A., & Alarcón, A. (2017). La lógica difusa en la modelización del riesgo operacional. Una solución desde la inteligencia artifical cubana. *Cofín Habana, 12*(2), 122-135. Obtenido de http://www.cofinhab.uh.cu/index.php/RCCF/article/view/232/224

Galán, J., & Venegas, F. (2016). Impacto de los medios electrónicos de pago sobre la demanda de dinero. *Investigación Económica, 75*(295), 93-124. Obtenido de http://www.redalyc.org/pdf/601/60144179003.pdf

Gil, V., & Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica, 22*(2), 193-197. Obtenido de http://www.redalyc.org/pdf/849/84953103011.pdf

González, P. (20 de Mayo de 2017). La banca ofrece más servicios en línea. *Diario El Comercio*.

Hernández, A. (2010). *Auditoría Informática y Gestión de Tecnologías De Información y Comunicación (TICs)*. Venezuela: Universidad Centroccidental Lisandro Alvarado.

Layva, K., Alarcón, L., & Ortegón, L. (2016). Exploración del diseño y arquitectura web. Aplicación a páginas electrónicas del sector bancario desde la perspectiva del usuario. *Revista Escuela de Administración de Negocios*(80), 41-57. Obtenido de http://www.redalyc.org/pdf/206/20645903004.pdf

López, M., Albanese, D., & Sánchez, M. (2014). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. *Contaduría y Administración, 59*(3), 61-88. Obtenido de https://core.ac.uk/download/pdf/25651585.pdf

López, S. (2013). Expansión internacional de los conglomerados financieros colombianos: retos para la supervisión. *Revista de Derecho Privado*(50), 1-38. Obtenido de http://www.redalyc.org/pdf/3600/360033221001.pdf

Martínez, Y., Blanco, B., & Loy, L. (2013). Propuesta del Sistema de Acciones para la implementación de la Auditoría con Informática. *Revista de Arquitectura e Ingeniería, 7*(2), 1-13. Obtenido de http://www.redalyc.org/pdf/1939/193929227003.pdf

Martínez, Y., Blanco, B., & Loy, L. (2013). Propuesta del Sistema de Acciones para la implementación de la Auditoría con Informática. *Revista de Arquitectura e Ingeniería, 7*(2), 1-13. Obtenido de http://www.redalyc.org/pdf/1939/193929227003.pdf

Muñoz, F., Sánchez, J., & Luque, T. (2014). Las estructuras basadas enla institución como determinantes de la confianza hacia la banca. *Revista de Estudios Empresariales. Segunda época*(2), 113-141. Obtenido de https://revistaselectronicas.ujaen.es/index.php/REE/article/view/1202/1897

Stable, Y. (2012). Auditoría de información y conocimiento en la organización. *Ingeniería Industrial, 23*(3), 260-271. Obtenido de http://www.redalyc.org/pdf/3604/360433581006.pdf

Vega, L., & Nieves, A. (2016). Procedimiento para la Gestión de la Supervisión y Monitoreo del Control Interno. *Ciencias Holguín, 22*(1), 1-19. Obtenido de http://www.redalyc.org/pdf/1815/181543577007.pdf

ANEXOS

Cuestionario para usuarios de la Banca Virtual del Banco Pichincha

1. ¿Conoce el uso de la Banca Virtual del Banco Pichincha?

Si

No

2. ¿Conoce los aspectos claves que le permitan identificar la información oficial del Banco Pichincha recibida en su correo y celular?

Si

No

3. ¿Su cuenta ha sido bloqueada por que Ud. ingreso mal la clave?

Si

No

4. ¿Identifica los sitios seguros para hacer transacciones?

Si

No

5. ¿Considera que su información y transacciones se encuentra lo suficientemente protegida?

Si

No