UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA ADMINISTRATIVA

TÍTULO DE INGENIERO EN
ADMINISTRACIÓN EN BANCA Y FINANZAS

Medidas de control y seguridad aplicados por los bancos frente a los fraudes electrónicos.

TRABAJO DE TITULACIÓN

AUTORA: Sarango Paucar, Elisa del Cisne

DIRECTORA: Salas Tenezaca, Eulalia Elizabeth, Mgs

LOJA - ECUADOR

2015

Septiembre, 2015

APROBACIÓN DEL DIRECTOR DEL TRABAJO DE TITULACIÓN

Magister.

Salas Tenezaca Eulalia Elizabeth

DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de titulación: Medidas de control y seguridad aplicados por los Bancos frente a los fraudes electrónicos, realizado por Sarango Paucar Elisa del Cisne, ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, julio de 2015

f). . . . . .

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo Sarango Paucar Elisa del Cisne declaro ser autora del presente trabajo de titulación: Medidas de control y seguridad aplicados por los Bancos frente a los fraudes electrónicos, de la Titulación de Ingeniero en Administración en Banca y Finanzas, siendo la Mgs. Elizabeth Salas directora del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado o trabajos de titulación que se realicen con el apoyo financiero, académico o institucional (operativo) de la Universidad"

f).....

Autora: Sarango Paucar Elisa del Cisne

Cédula: 1104679483

DEDICATORIA

A Dios, sobre todas las cosas por darnos a mi familia y a mi salud, que es la fuente fundamental para cumplir nuestros objetivos, el resto viene por añadidura fruto del esfuerzo, constancia y dedicación.

A mi amado esposo, por la paciencia y comprensión en cada instante de nuestras vidas y **a nuestro hijo** Alejandrito por darnos la mayor felicidad de nuestras vidas y brindarnos una familia hermosa.

AGRADECIMIENTO

A la Universidad Técnica Particular de Loja, que a través de la Titulación de Banca y Finanzas y su personal docente nos impartieron de conocimientos y experiencias con responsabilidad, para formarnos profesionalmente y permitir que nuestras metas profesionales sean posibles.

Así mismo a mi Directora de tesis Mgs. Elizabeth Salas quién me brindó su apoyo en todas las etapas del desarrollo del presente proyecto.

INDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Actualmente las instituciones financieras se encuentran expuestas a posibles fraudes y ataques en los canales electrónicos, que pueden ocasionar perdidas si no se toman las medidas de seguridad necesarias, por lo que la Junta Bancaria ha emitido la resolución JB-2012-2148 con la finalidad de dar los lineamientos generales que permitan a las IFIS asegurar sus canales electrónicos, pero esto no garantiza que se llegue a tener un 100% de seguridad, es por eso que cada institución ha adoptado mecanismos que permitan asegurar sus canales manteniendo el balance con la usabilidad de sus sistemas de tal forma que dichos mecanismos no hagan desertar a los clientes del uso del canal.

PALABRAS CLAVES: Basilea, Canales electrónicos, Fraudes electrónicos, Resolución JB-2012- 2148, Seguridad lógica y física.

ABSTRACT

Currently financial institutions are exposed to possible fraud and attacks on electronic channels, which can cause losses if the necessary precautions are taken, so the Banking Board issued Resolution JB-2012-2148 in order to give general guidelines that allow IFIS secure their electronic channels, but does not guarantee it gets to have 100% security, that is why each institution has adopted mechanisms to ensure its canals maintaining balance with usability their systems so that these mechanisms do not defecting customers use the channel.

KEYWORDS: Basel, Feeds, phishing, Resolution JB-2012- 2148, logical and physical security.

INTRODUCCIÓN

El presente trabajo pretende identificar los mecanismos utilizados por los Bancos para asegurar los canales electrónicos, lo cual viene vinculado con la capacitación al usuario. Una plataforma segura no garantiza que el usuario deje de sufrir fraudes que les ocasione pérdida de dinero, razón por la cual con este trabajo se pretende determinar los fraudes más frecuentes en canales electrónicos así como el nivel de cumplimiento de los lineamientos establecidos por el comité de la Basilea, resolución JB-2012-2148 y el nivel de capacitación brindado a los usuarios.

De igual forma por los fraudes electrónicos existen pérdidas económicas de las instituciones, dado que si se determina que la responsabilidad no es del cliente la institución financiera debe cubrir los valores comprometidos, adicionalmente existen mecanismos de cambio de responsabilidad entre instituciones en donde la institución que no cumple con las seguridades debe asumir los riesgos.

CAPÍTULO I: ESTADO DEL ARTE

1.1 Canales electrónicos

Las instituciones financieras con la finalidad de disminuir costos operativos de uso de canal físico y así mismo con el objetivo de ofrecer canales alternativos que le permita transaccionar a sus clientes desde cualquier lugar en donde se encuentren han implementado canales alternativos a los físicos denominados canales electrónicos.

1.1.1 Definición de canal electrónico.

Un canal electrónico es aquel que se puede utilizar para realizar una transacción de compra, venta, consulta requerida por el cliente sin necesidad de la intervención del factor humano.

Un canal electrónico es un concepto genérico aplicable a cualquier tipo de negocio, sin embargo para el presente trabajo se enfocará este concepto al negocio de las instituciones financieras.
Los canales electrónicos han surgido con la finalidad de dar mecanismos alternativos para transaccionar a los clientes obteniendo los siguientes beneficios:

- Disminución de tiempo para el cliente en sus transacciones.
- Eliminación de colas para transaccionar.
- Disminución de gastos de operación dado que el costo de transacción en canal electrónico es menor al de un canal físico.
- Facilidad de distribución para ubicar canales en el mercado.
- Comodidad para el cliente al permitirle transaccionar a cualquier hora del día, en el lugar que se encuentre siempre y cuando exista cobertura dependiendo del tipo de canal.

De igual manera este tipo de canales tienen ciertas debilidades en torno a temas de seguridad ya que son vulnerables en varios casos. Muchos de estos puntos de seguridad pueden ser resueltos por los departamentos de tecnología de las instituciones financieras o por medio de consultorías especializadas que permitan implementar las seguridades necesarias.

Por más seguridades que se implementen no se logrará tener un canal 100% seguro debido a que las tecnologías evolucionan constantemente y así mismo existe una brecha cultural en nuestro país que hace que los clientes sean engañados por terceros para obtener las

credenciales y medios de acceso a los canales con lo cual se realizan fraudes sobre sus cuentas.

1.1.2 Tipos de canales electrónicos.

Existen varios tipos de canales electrónicos implementados en las instituciones financieras del país, y también se los conoce como canales de Banca Electrónica aunque en nuestro medio el término banca electrónica se utiliza para nombrar a la banca por internet, de los canales más comunes se tiene los siguientes:

1.1.2.1 *Banca telefónica o canal telemático*.

Este tipo de canal le permite al cliente realizar transacciones financieras mediante el uso de teléfono realizando una llamada a los números provistos por su institución financiera, normalmente para acceder a este tipo de canal se requiere de una credencial de acceso o en su defecto pasar por preguntas de verificación las cuales se realizan de manera automática, una vez que el sistema reconoce al cliente le permite por medio de menús numéricos realizar las transacciones sean estas de consulta, servicios o monetarias.

Ilustración 1: Banca telefónica o canal telemático

Fuente: Web Grupo BBVA

Las transacciones más comunes que se pueden realizar en este tipo de canal son:

- Consultas: Transacciones para consultas generales de saldos de cuentas, movimientos, valores por pagar de créditos, consulta de inversiones.

- Servicios: Activación y bloqueo de tarjetas, Anulación, suspensión, revocatoria de cheques, Solicito de chequeras, obtención de claves de tarjetas de débito, crédito.

1.1.2.2 *Banca por internet*.

Conocida también con los nombres de Banca Virtual, Banca en Línea es un medio que permite a los clientes de las instituciones financieras realizar transacciones sobre sus cuentas de ahorros, corrientes mediante el uso del internet para acceder al canal.

El beneficio de este tipo de canal es que los clientes pueden transaccionar 24X7[1] todos los días del año desde el lugar en donde se encuentre.

La banca virtual se encuentra categorizada en el segmento B2C[2] dentro del comercio electrónico.

Ilustración 2: Banca por internet

Fuente: Sitio Web Banco de Loja

Los principales tipos de transacción que se pueden realizar en este canal son:

- Transferencia de fondos entre cuentas propias, del mismo banco u otras instituciones financieras por medio del sistema de pagos SPI[3].

[1] 24 horas al día, los 7 días a la semana.
[2] B2C (Negocio a Consumidor)
[3] SPI (Sistema de pagos interbancarios)

- Consultas de saldos de cuentas de ahorros corrientes, consulta de créditos, inversiones, tarjetas de crédito.
- Pagos de servicios de instituciones públicas y privadas.
- Bloqueos/Anulaciones de cuentas, tarjetas, canales, cheques.
- Solicitudes de cuentas, claves, tarjetas.
- Apertura de inversiones.
- Recarga de servicios celular, televisión prepagada entre otros.

1.1.2.3 *Cajeros automáticos o ATM*[4].

Un cajero automático es un equipo que posee un computador integrado y que permite realizar transacciones financieras mediante el uso de una tarjeta que le autoriza al cliente a transaccionar.

Existen dos tipos de estos equipos que son los que únicamente dispensan efectivo y los que adicionalmente permite recibir efectivo para depósito.

Este tipo de canal tiene límites para transaccionar y son los que menos cantidad de dinero permiten en sus transacciones
Las transacciones comunes en cajeros automáticos son:

- Retiro de efectivo.
- Consulta de saldos.
- Transferencias entre cuentas propias.

Ilustración 3: Cajeros automáticos o ATM[5]

Fuente: Banco Pichincha

[4] ATM(Automated Teller Machine)
[5] ATM(Automated Teller Machine)

1.1.2.4 *Banca celular*.

Por medio de este canal se permite realizar transacciones con el uso del teléfono celular registrado por el cliente, este canal se divide en 4 tipos de acuerdo a su mecanismo de acceso y tecnología.

- **Banca SMS:** Este tipo de banca permite transaccionar desde el celular mediante el uso de mensajes de texto, la desventaja principal es que el cliente debe aprender códigos cortos para poder hacer sus transacciones lo cual ha hecho que el canal no se use masivamente.

Ilustración 4: Banca celular

Fuente: Banco Provincial

- **Banca WAP/HTML5:** Esta banca se puede acceder desde el navegador del teléfono celular y se adapta a cada tipo de equipo, la desventaja es que normalmente por su interfaz gráfica no es muy sencilla de usar y además requiere de que el cliente disponga de un plan de datos o conexión wi-fi

Ilustración 5: Banca WAP/HTML5

Fuente: Banco Provincial

- **Banca USSD:** Es el canal mediante la marcación de un código corto por ejemplo *123# permite acceder a un menú transaccional de servicios financieros.

Ilustración 6: Banca USSD

Fuente: (Zweicon)

- **Banca APP:** Este tipo de Banca se instala como aplicación en el teléfono celular y está disponible por cada tipo de sistema operativo Smart Phone como es el caso Iphone, Android, Blackberry, Windows Phone.

El cliente requiere de plan de datos o wi-fi y de un Smart Phone para poder utilizar este servicio.

Ilustración 7: Banca APP

Fuente: Sitio Web Banco Bolivariano

Las principales transacciones de este tipo de Canal son:

- Transferencia de fondos entre cuentas propias, del mismo banco u otras instituciones financieras por medio del sistema de pagos SPI[6].
- Consultas de saldos de cuentas, tarjetas de crédito, créditos e inversiones.
- Pagos de servicios básicos
- Bloqueos/Anulaciones de cuentas, tarjetas, canales, cheques.
- Recarga de servicios celular, televisión prepagada entre otros.

1.1.2.5 *Kioskos electrónicos*.

Los kioskos electrónicos es un canal que normalmente se encuentra disponible dentro de oficinas físicas, es un equipo que permite realizar normalmente transacciones de consulta.

Las transacciones que se realizan en este tipo de dispositivo son muy variadas entre cada institución pero la tendencia es a realizar transacciones de consulta que permitan disminuir las transacciones realizar por personal de las instituciones.

1.1.3 Tipos de canales electrónicos en las instituciones financieras del país.

En base a la información obtenida de la Superintendencia de Bancos del Ecuador (SIB) año 2014, en el país existen 27 Bancos y 39 cooperativas reguladas por el organismo en mención. La cuales están clasificadas por los activos que disponen en: grandes, medianas y pequeñas; y, en el caso de las cooperativas también existe la clasificación muy pequeñas, esta distribución se muestran en las tablas siguientes:

Tabla 1: Tipos de Bancos Año 2014

TIPO DE BANCO	# DE INSTITUCIONES
BANCOS PRIVADOS GRANDES	4
BANCOS PRIVADOS MEDIANOS	7
BANCOS PRIVADOS PEQUEÑOS	16
TOTAL BANCOS	27

Fuente: Superintendencia de bancos del ecuador año 2014

Elaborado por: Elisa Sarango

[6] SPI (Sistema de pagos interbancarios)

Tabla 2: Tipos de Cooperativas Año 2014

TIPO DE COOPERATIVA	# DE INSTITUCIONES
COO GRANDES	3
COO MEDIANAS	8
COO MUY PEQUEÑAS	12
COO PEQUEÑAS	16
TOTAL COOPERATIVAS	39

Fuente: Superintendencia de bancos

Elaborado por: Elisa Sarango

No existe información en la SIB que presente los canales electrónicos disponibles por cada institución es por eso que se ha realizado el trabajo de investigación mediante consultas en la web para obtener los canales disponibles por cada una de las instituciones y se presenta el resumen en la siguiente tabla:

Tabla 3: Canales Electrónicos de Bancos Año 2014

BANCO	ATM	Banca Móvil	Banca Telefónica	Banca Virtual
GUAYAQUIL	SI	SI	SI	SI
PACIFICO	SI	SI	SI	SI
PICHINCHA	SI	SI	SI	SI
PRODUBANCO	SI	SI	SI	SI
AUSTRO	SI	SI	SI	SI
BOLIVARIANO	SI	SI	SI	SI
SOLIDARIO	SI	SI	SI	SI
GENERAL RUMIÑAHUI	SI	SI	SI	SI
INTERNACIONAL	SI	SI	SI	SI
MACHALA	SI	NO	SI	SI
PROMERICA	SI	NO	NO	SI
AMAZONAS	SI	SI	SI	SI
COFIEC	SI	NO	NO	SI
COMERCIAL DE MANABI	SI	NO	NO	SI
LITORAL	SI	NO	NO	NO
LOJA	SI	NO	SI	SI

CITIBANK	SI	SI	SI	SI
SUDAMERICANO	SI	NO	NO	SI
UNIBANCO	SI	SI	SI	SI
COOPNACIONAL	SI	NO	NO	NO
PROCREDIT	SI	NO	NO	SI
CAPITAL	SI	NO	NO	SI
FINCA	SI	NO	NO	NO
DELBANK	SI	NO	NO	SI
D-MIRO S.A.	SI	NO	NO	NO
	100%	48%	60%	84%

Fuente: Sitios web de las instituciones financieras

Elaborado por: Elisa Sarango

En base a los datos expuestos de los bancos se puede evidenciar que todos los Bancos disponen de cajeros automáticos, el 84% poseen Banca Virtual, un 60% Banca Telefónica y un 48% Banca Móvil, de ahí que el canal que se encuentra mayormente masificado en nuestro país son los cajero automáticos.

Tabla 4: Canales Electrónicos de Cooperativas Año 2014

COPERATIVAS	ATM	Banca Móvil	Banca Telefónica	Banca Virtual
JUVENTUD ECUATORIANA PROGRESISTA	SI	NO	NO	SI
JARDIN AZUAYO	SI	NO	NO	SI
29 DE OCTUBRE	SI	NO	NO	SI
COOPROGRESO	SI	NO	NO	SI
MEGO	SI	NO	NO	SI
RIOBAMBA	SI	NO	NO	NO
OSCUS	SI	NO	NO	NO
SAN FRANCISCO	SI	NO	NO	NO
CACPECO	SI	NO	NO	NO
ANDALUCIA	SI	NO	NO	SI
MUSHUC RUNA	SI	NO	NO	NO
15 DE ABRIL	SI	NO	NO	NO
EL SAGRARIO	SI	NO	NO	SI
23 DE JULIO	SI	NO	NO	NO
CODESARROLLO	NO	NO	NO	NO
ATUNTAQUI	SI	NO	NO	NO
ALIANZA DEL VALLE	SI	NO	NO	SI
CAMARA DE COMERCIO DE	SI	NO	NO	SI

AMBATO				
SANTA ROSA	SI	NO	NO	NO
PABLO MUÑOZ VEGA	SI	NO	NO	SI
CONSTRUCCION COMERCIO Y PRODUCCION LTDA	SI	NO	NO	NO
TULCAN	SI	SI	NO	SI
CACPE BIBLIAN	SI	NO	NO	NO
SAN JOSE	SI	NO	NO	NO
CACPE PASTAZA	SI	NO	NO	NO
PADRE JULIAN LORENTE	SI	NO	NO	NO
CACPE LOJA	SI	NO	NO	NO
COMERCIO	SI	NO	NO	NO
CHONE LTDA	SI	NO	NO	NO
SAN FRANCISCO DE ASIS	NO	NO	NO	NO
GUARANDA	SI	NO	NO	NO
11 DE JUNIO	SI	NO	NO	NO
COTOCOLLAO	SI	NO	NO	NO
LA DOLOROSA	SI	NO	NO	NO
COOPAD	SI	NO	NO	NO
CALCETA	NO	NO	NO	NO
9 DE OCTUBRE	SI	NO	NO	NO
SANTA ANA	NO	NO	NO	NO
SAN PEDRO DE TABOADA	NO	NO	NO	NO
	87%	3%	0%	28%

Fuente: Sitios web de las instituciones financieras

Elaborado por: Elisa Sarango

En base a la información adjunta se puede evidenciar que la mayor parte de cooperativas no tienen implementados Banca Celular, Banca Virtual y Banca telefónica, esto puede obedecer a la cultura de los clientes con los cuales cuentan, a las limitantes de la infraestructura tecnológica, entre otros aspectos.

1.2 Fraudes

1.2.1 Que son los fraudes.

El fraude se define como el engaño del cual se vale una persona para hacerse de un objeto de procedencia ajena en perjuicio de otra, y de acuerdo a la definición legal de nuestro país un engaño es la acción contraria a la verdad o a la rectitud. Calificación jurídica de la

conducta consistente en una maquinación o subterfugio insidioso tendiente a la obtención de un provecho ilícito.

Así mismo un fraude electrónico es la actividad por la cual las personas toman acciones mediante equipos o recursos informáticos para obtener una ventaja en este caso económica sobre otra persona por medio de engaños.

1.2.1 Tipos de fraudes en canales electrónicos.

Existen varios tipos fraudes electrónicos de los cuales se van a describir los más comunes aplicados en nuestro país.

1.2.1.1 *Skimming*.

Según Chávez J (2012) el Skimming es el mecanismo mediante el cual se roba la información de tarjetas de crédito o débito del cliente al momento en que este está realizando la transacción, estos robos más comunes se realizan en gasolineras, restaurantes, bares y se da cuando uno pierde la tarjeta de crédito de vista, así mismo se lo realiza en los cajeros automáticos.

Por lo general se coloca un dispositivo adicional sobre el cajero automático o lector de tarjeta con el cual se copia la información de la tarjeta y se coloca dispositivos adicionales para obtener el PIN o la clave de la tarjeta.

1.2.1.2 *Phishing*.

Según Chávez J (2012) el phising también llamado suplantación de identidad consiste en hacer que los clientes ingresen a sitios web falsos en donde se solicita el ingreso de información de credenciales y mecanismos de validación del sitio, los cuales son utilizados posteriormente por los atacantes para realizar movimientos de dinero de las cuentas de las víctimas.

Este tipo de fraudes normalmente se realiza aplicando ingeniería social, es decir se remite correos a los clientes aparentando ser de fuente confiable es decir de su propio banco, el

contenido del correo normalmente indica que gano el premio, que los datos deben ser actualizados o la cuenta será bloqueada entre otros.

1.2.1.3 *Pharming*.

Según Chávez J (2012) es un mecanismo que consiste en aprovechar vulnerabilidades de los servidores o equipos de los usuarios para direccionar a los clientes a sitios fraudulentos, por ejemplo si alguien ingresa a www.pichincha.com lo redireccionan a otra ruta que contiene un sitio clonado y solicitan información del cliente que posteriormente usaran para realizar fraude.

1.2.1.4 *Keylogger, Screenlogger, MouseLogger*.

Según Chavez J (2012) son técnicas que espían en el computador del cliente y la almacenan cuando el cliente presiona las teclas, mueve el mouse, estas técnicas normalmente se aplican en sitios de internet públicos como cybercafes.

1.2.2 Ejemplos de fraudes en canales electrónicos.

A continuación se presentan algunos ejemplos de fraudes en canales electrónicos realizados en bancos de nuestro país.

1.2.2.1 *Phishing a institución financiera ecuatoriana*.

El banco analizado dispone de Banca virtual, la cual para transaccionar requiere de los siguientes mecanismos de seguridad:

- Identificación del cliente (Cédula/RUC/Pasaporte).
- Clave de acceso proporcionada por la institución.
- Preguntas de seguridad.
- Tarjetas de coordenadas para validación de transacciones.
- Requiere que el cliente acceda a su correo electrónico para confirmación de transacciones.

De esta forma para poder realizar phishing los atacantes debe obtener todos los datos indicados.

Paso 1: Correo remitido por el atacante y recibido por el cliente

ESTIMADO CLIENTE [redacted]

[redacted]BANCO le comunica que nuestros servidores de procesos bancarios han sido actualizados (sic) y estan ya operativos

Sin embargo debido a la ingente cantidad de usuarios que usan Internet como medio de pago seguro, nos vemos en la obligación de pedirle su colaboración para una rápida restauracion de los datos en las nuevas plataformas.

Tiempo de valides para la confirmación es de 24 horas se ruega lo haga de inmediato para evitar el posible cierre de su cuenta y la futura pérdida de datos.

Puede entrar a su cuenta haciendo click sobre el enlace correspondiente . Con esta acción su cuenta quedará actualizada de forma permanente.

INGRESE A NUESTRA BANCA POR INTERNET

[redacted] pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnolog:a en protección y encriptación de datos.

Banco [redacted] S.A

https://www.[redacted]banco.com/GFPNet/

Todos los Derechos Reservados [redacted]

Para cualquier duda o aclaración comun?quese con nosotros al Tel. 1 226 3990 o 800 110 3990

Ilustración 8: E-mail remitido por el atacante

Fuente: Sitio web para realizar fraude

Paso 2: Luego de acceder el cliente visualiza la página principal de la institución de manera natural sin darse cuenta que es un sitio clonado y que luce igual.

Ilustración 9: Sitio clonado

Fuente: Sitio web para realizar fraude

Paso 3: Ingresa a la banca virtual.

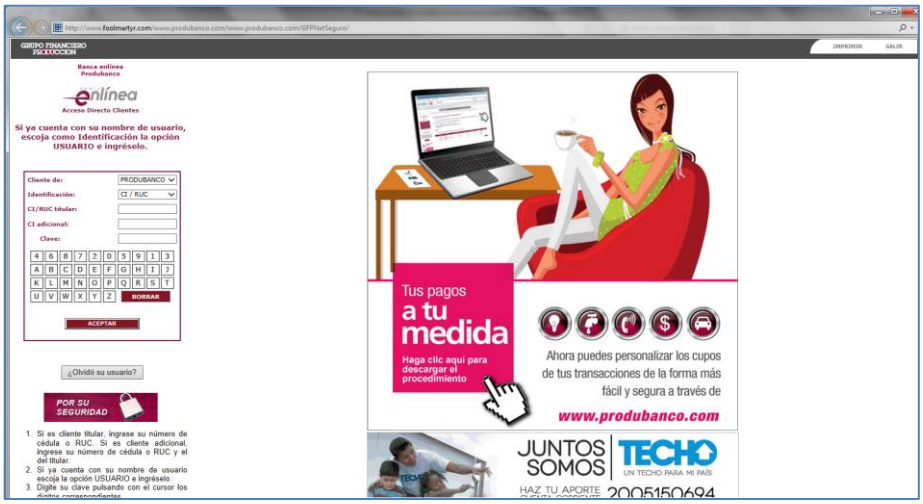


Ilustración 10: Sitio de acceso a banca virtual

Fuente: Sitio Web Ficticio

El cliente no se da cuenta que está ingresando a una dirección web que no es la correcta, en este caso esta dirección.

Ilustración 11: Link de acceso ficticio

Ingresa su identificación y clave.

Ilustración 12: Datos de acceso la banca virtual

Fuente: Sitio Web Ficticio

Paso 4: Le solicita el ingreso de sus datos de la tarjeta de coordenadas.

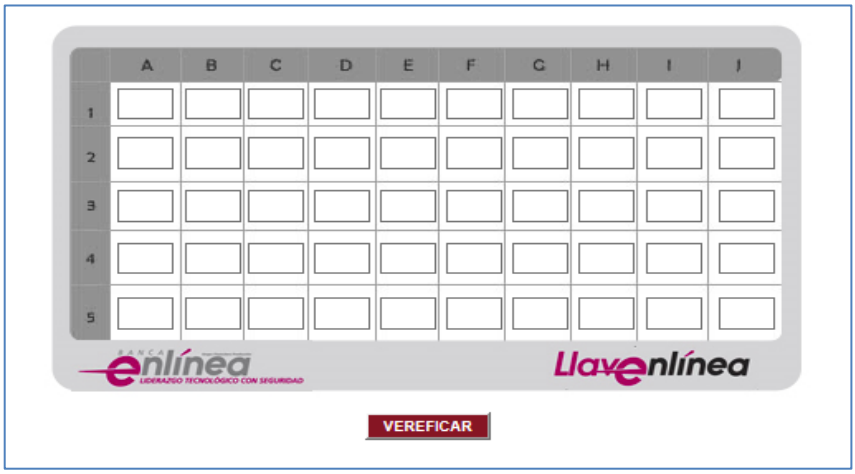


Ilustración 13: Solicita datos de tarjeta de coordenadas

Fuente: Sitio Web Ficticio

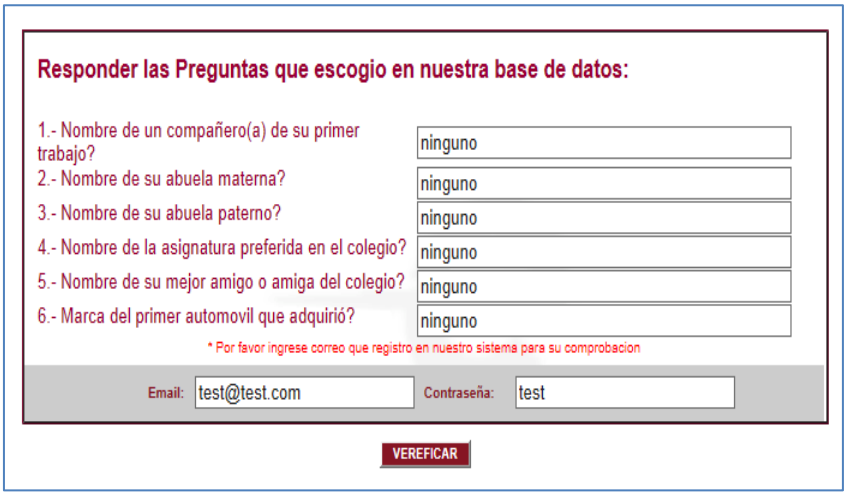


Ilustración 14: Datos de preguntas de verificación

Fuente: Sitio Web creado por grupos de fraudes

Paso 5: Luego confirma que se ha recibido la información

Ilustración 15: Datos de confirmación que remite el sitio falso

Fuente: Sitio Web Ficticio

El cliente sin darse cuenta proporciono todos sus datos confidenciales de acceso a banca virtual con lo cual el atacante procede a realizar transacciones desde su cuenta para realizar el fraude.

1.2.2.2 *Proceso de Skimming*.

Se presenta los pasos para realizar skimming, cabe indicar que las fotografías han sido tomadas del sitio web (Slayer).

Paso 1: Colocan una lectora sobrepuesta la cual se encarga de obtener los datos de la banda magnética de las tarjetas. Normalmente la adaptan al color del cajero automático.

Ilustración 16: Montaje de lectora falsa

Fuente: www.hoax-slayer.com

Paso 2: El cajero se encuentra con la lectora sobrepuesta, a simple vista no se visualiza la diferencia.

Ilustración 17: Lectora sobrepuesta

Fuente: www.hoax-slayer.com

Paso 3: Colocan una cámara para grabar las pulsaciones del teclado y obtener la clave.

Ilustración 18: Mecanismo para colocar la cámara

Fuente: www.hoax-slayer.com

Ilustración 19: Cámara para obtención de clave

Fuente: www.hoax-slayer.com

Paso 4: Posteriormente con la información obtenida proceden a grabar las bandas en tarjetas vírgenes y registra en papel la clave.

Con esto proceden a realizar retiros en los cajeros automáticos normalmente de entidad diferente a la que realizaron la clonación y tiene identificadas ubicaciones en donde no existen cámaras.

1.3 Seguridad

1.3.1 La seguridad informática.

Según Aguirre J (2006) la seguridad informática se define como “Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico”

Existe un concepto más amplio que es la seguridad de la información la cual se constituye en un conjunto de acciones o medidas de prevención en las organizaciones y en los sistemas que usan tecnología para proteger la información y que esta mantenga su integridad, confidencialidad y disponibilidad requerida.

Cuando se habla de integridad esto corresponde a mantener la información original y que esta no sufra cambios no autorizados que distorsionen el sentido de la misma.

La disponibilidad corresponde a la acción de tener la información de manera oportuna sin interrupciones a las personas autorizadas a la misma.

Y la confidencialidad se refiere a que la información no puede ser divulgada o accedida por usuarios no autorizados.

Cuando se habla de seguridad en los canales esta se refiere a los medios implementados para garantizar que los canales sean seguros sin que esto signifique que sean inutilizables ya que el aplicar mecanismos de seguridad también implica poner mayores complicaciones de acceso a los canales lo cual puede ocasionar una deserción de uso de los mismo por parte de los clientes de ahí que se deben implementar las técnicas adecuadas para mantener el equilibrio.

1.3.2 Seguridad lógica de los canales.

La seguridad lógica se refiere a todos los medios que se pueden controlar a nivel de aplicaciones de software como restringir acceso a los programas y archivos, esta seguridad

también debe ser aplicada desde el desarrollo de los aplicativos en donde se deben aplicar técnicas de seguridad.

Dentro de las recomendación de seguridad para el desarrollo de aplicaciones web se tienen las OWASP[7], las cuales dan los lineamientos para el desarrollo de aplicaciones web en este caso Bancas Virtuales, el cual es uno de los puntos a considerar para la seguridad.

1.3.3 Seguridad física.

La seguridad física está enfocada a proteger el recurso físico del sistema como por ejemplo en la instalación de un cajero automático puede ser:

- Sitio de instalación, elementos adicionales como cámaras de seguridad.
- Anclaje del cajero al piso
- Protocolos de aprovisionamiento de dinero.
- Seguridad antifraude, como barras físicas, componente anti-skimming

Entre otros elementos de seguridad que deben ser aplicados en base a las normativas locales como la resolución de la Junta BancariaJB-2012-2148, PCI[8], ISO-27000[9] entre otras.

[7] OWASP (The Open Web Application Security Project)
[8] PCI (Estándar de seguridad de datos para la industria de tarjetas de pago)
[9] ISO-27000 (Normas de seguridad aplicadas por la ISO)

CAPÍTULO II: NORMATIVAS NACIONALES E INTERNACIONALES PARA PREVENCIÓN DE FRAUDES EN CANALES ELECTRÓNICOS

2.1 Normas y mejores prácticas de organismos internacionales.

Con la finalidad de prevenir el fraude en las instituciones financieras los organismos de controles nacionales e internacionales han desarrollado un conjunto de lineamientos y normativas que deben ser implementas en algunos casos de manera obligatoria y en otros queda a discreción de cada institución.

2.1.1 Acuerdos de basilea.

El comité de la Basilea se establece en el año 1975, por los presidentes de los Bancos Centrales llamado en su momento G10[10], se reúnen con la finalidad de establecer lineamientos de regulación, supervisión. Actualmente los países miembros del comité son Basilea, Alemania, Italia, Canadá, Francia, Holanda, España, Japón, Luxemburgo, Estados Unidos, Reino Unido, Suiza, Suecia.
Al momento los acuerdo de Basilea establecidos se han dado en los años 1988 con la Basilea I, 2004 Basilea II y 2010 la Basilea III.

En la Basilea I se establecen los principios en los que debe fundamentar la actividad Bancaria como el capital regulatorio, requisito de permanencia, capacidad de absorción de pérdidas y protección ante la quiebra. En esta fundamentación el capital tiene que ser suficiente para enfrentar los riesgos producto del giro del negocio como son los crédito, el mercado y tipos de cambio, y el capital mínimo de la entidad bancaria debía ser el 8% del total de los activos de riesgo, estos lineamientos no tenían en consideración el riesgo crediticio de acuerdo al tipo de deudor con lo cual no se establecía mecanismos para la evaluación de la calidad crediticia.
En el acuerdo de la Basilea II, se desarrolla el tema del cálculo de los activos ponderados por riesgo, lo cual permite a las instituciones financieras aplicar modelos de calificación de riesgo en base a modelos internos.

Mientras que la Basilea I se basaba en un solo pilar de requerimientos mínimos de capital, la Basilea II toma tres pilares que son los requerimientos mínimos de capital, revisión de la entidad supervisora y disciplina del mercado.

[10] G10 Grupo de 10 países

En este acuerdo de la Basilea II ya se considera el riesgo operacional, hay que considerar que el riesgo operativo incluye de manera indirecta a los canales electrónicos sin tener en ese momento ningún tipo de lineamiento.

Los Acuerdos de la Basilea III la cual se inició el 2010, contiene los siguientes lineamientos:

- Aumento de la calidad del capital para asegurar mayor capacidad para absorber perdidas.
- Establecimientos de reservas de capital en momentos buenos del ciclo que puedan ser utilizados en momentos de recesión.
- Introducción de un ratio de apalancamiento como una medida complementaria al ratio de solvencia basada en riesgo.
- Aumento del nivel de los requerimientos de capital, para fortalecer la solvencia de las entidades y contribuir a una mayor estabilidad financiera.
- Mejoras de los fundamentos 2 y 3, se establecen guías en las áreas como gestión del riesgo de liquidez, buenas prácticas para la valoración de instrumentos financieros, ejercicios de estrés, gobierno corporativo y remuneración.
- Introducción de un estándar de liquidez.

En la siguiente tabla se resumen los 29 principios básicos de la Basilea III tomados de (Basilea).

Tabla 5: Principios de la Basilea III

Nombre	Principio
Principio 1 – Atribuciones, objetivos y potestades	El sistema de supervisión bancaria cuenta con atribuciones y objetivos claros para cada participante, concediéndole a través de un marco jurídico las siguientes potestades; Autorizar bancos, realizar una supervisión continua, asegurar el cumplimiento de la ley y adoptar medidas correctivas en materia de seguridad y solvencia
Principio 2 – Independencia, rendición de cuentas, recursos y protección legal de los supervisores	El supervisor bancario contará con independencia operativa, procesos transparentes, gobierno corporativo y recursos adecuados, además rendirá cuentas del desempeño de sus funciones

Principio 3 – Cooperación y colaboración	Las leyes, regulaciones y otros procedimientos facilitan la aportación y colaboración de las autoridades locales y extranjeras para mantener la información confidencial
Principio 4 – Actividades permitidas	Las actividades que pueden desarrollar las entidades financieras son claramente definidas y se controlará la palabra "banco" como razón social
Principio 5 – Criterios para la concesión de licencias	Los establecimientos que no cumplan con los criterios asignados por la autoridad encargada de autorizar las licencias de un establecimiento, este tendrá la potestad de negarlo
Principio 6 – Cambio de titularidad de participaciones significativas	El supervisor tiene la autoridad para examinar, rechazar y establecer condiciones prudenciales en lo que se refiere a propuestas de cambio de titularidad de participaciones sean estas directas o indirectas
Principio 7 – Adquisiciones sustanciales	El supervisor puede autorizar, rechazar, recomendar y establecer condiciones prudenciales para las adquisiciones o inversiones que realice el banco
Principio 8 – Enfoque supervisor	El supervisor deberá mantener una evaluación prospectiva del perfil de riesgo de una o un grupo de entidades financieras, con la finalidad de que se pueda identificar, evaluar, los riesgos procedentes del sistema bancario y adoptar las medidas correspondientes
Principio 9 – Técnicas y herramientas de supervisión	El supervisor utiliza una adecuada gama de técnicas y herramientas y emplea los recursos de manera proporcionada teniendo en cuenta el perfil de riesgo y la importancia sistémica de los bancos
Principio 10 – Informes de supervisión	El supervisor se encargara de revisar, analizar y verificar los informes de los bancos, a través de inspecciones in situ o con la ayuda de expertos externos
Principio 11 – Potestades correctivas y sancionadoras del supervisor	El supervisor tiene una variedad de herramientas de supervisión que le permite aplicar adecuadas medidas correctivas a actividades que podrían generar riesgos para las entidades financieras
Principio 12 – Supervisión	El supervisor deberá llevar su labor en base consolidada para todo el grupo bancario, y si corresponde aplicar normas

consolidada	prudenciales a todos los aspectos de las actividades que el grupo realiza a escala mundial
Principio 13 – Relaciones entre el supervisor de origen y el de destino	Los supervisores exigirán que las operaciones locales que realizan los bancos extranjeros se lleven a cabo aplicando las mismas normas que tienen las entidades locales
Principio 14 – Gobierno corporativo	Los supervisores se encargaran de confirmar que los bancos y grupos bancarios cuenten con políticas y procesos solidas en materia de gobierno corporativo
Principio 15 – Proceso de gestión del riesgo	El supervisor comprueba que los bancos cuenten con un proceso integral de gestión de riesgo, para identificar, cuantificar, evaluar, vigilar, informar y controlar todos los riesgos significativos en el momento oportuno
Principio 16 – Suficiencia de capital	El supervisor exige a los bancos unos requerimientos de capital prudentes y adecuados que reflejen los riesgos asumidos, y afrontados, por un banco en el contexto de la situación macroeconómica y de los mercados donde opera. El supervisor define los componentes del capital, teniendo en cuenta su capacidad para absorber pérdidas.
Principio 17 – Riesgo de crédito	El supervisor verifica que los bancos disponen de un adecuado proceso de gestión del riesgo de crédito que tiene en cuenta su apetito por el riesgo, su perfil de riesgo y la situación macroeconómica y de los mercados. Esto incluye políticas y procesos prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo de crédito (incluido el riesgo de crédito de contraparte) en el momento oportuno. El ciclo de vida completo del crédito deberá quedar contemplado, incluida la concesión del crédito, la evaluación del crédito y la gestión continua de las carteras de préstamos e inversiones
Principio 18 – Activos dudosos, provisiones y reservas	El supervisor verifica que los bancos cuentan con adecuadas políticas y procesos para una pronta identificación y gestión de los activos dudosos y para el mantenimiento de suficientes provisiones y reservas.

Principio 19 – Concentración de riesgos y límites de exposición a grandes riesgos	El supervisor verifica que los bancos cuentan con políticas y procesos adecuados para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar concentraciones de riesgo en el momento oportuno. Los supervisores establecen límites prudenciales que acotan las posiciones del banco frente a una misma contraparte o grupos de contrapartes vinculadas.
Principio 20 – Transacciones con partes vinculadas	A fin de evitar abusos en las transacciones con partes vinculadas y reducir el riesgo de un conflicto de intereses, el supervisor exige a los bancos realizar con total imparcialidad cualquier transacción con partes vinculadas; vigilar estas transacciones; adoptar medidas adecuadas para controlar o mitigar los riesgos; y reconocer contablemente las pérdidas en las exposiciones frente a partes vinculadas con arreglo a las políticas y procesos habituales.
Principio 21 – Riesgo país y riesgo de transferencia	El supervisor verifica que los bancos cuentan con políticas y procesos adecuados para identificar, cuantificar, evaluar, informar y controlar o mitigar el riesgo país y el riesgo de transferencia en sus préstamos e inversiones internacionales en el momento oportuno.
Principio 22 – Riesgo de mercado	El supervisor verifica que los bancos cuentan con un adecuado proceso de gestión del riesgo de mercado que tiene en cuenta su apetito por el riesgo, su perfil de riesgo, la situación macroeconómica y de los mercados y el riesgo de un deterioro sustancial de la liquidez de mercado. Esto incluye políticas y procesos prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar los riesgos de mercado en el momento oportuno.
Principio 23 – Riesgo de tasa de interés en la cartera de inversión	El supervisor verifica que los bancos cuentan con sistemas adecuados para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo de tasa de interés en la cartera de inversión en el momento oportuno. Estos sistemas tienen en cuenta el apetito por el riesgo y el perfil de riesgo del banco, así como la situación macroeconómica y de los mercados.

Principio 24 – Riesgo de liquidez	El supervisor exige a los bancos unos requerimientos de liquidez prudentes y adecuados (de tipo cuantitativo, cualitativo o de ambos tipos) que reflejen las necesidades de liquidez del banco. El supervisor verifica que los bancos disponen de una estrategia que les permite la gestión prudente del riesgo de liquidez y el cumplimiento de los requerimientos de liquidez. La estrategia tiene en cuenta el perfil de riesgo del banco, así como la situación macroeconómica y de los mercados, e incluye políticas y procesos prudentes, acordes con el apetito por el riesgo de la entidad, para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo de liquidez a lo largo de un conjunto relevante de horizontes temporales.
Principio 25 – Riesgo operacional	El supervisor verifica que los bancos cuentan con un marco adecuado de gestión del riesgo operacional que tiene en cuenta su apetito por el riesgo, su perfil de riesgo y la situación macroeconómica y de los mercados. Esto incluye políticas y procesos prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo operacional en el momento oportuno.
Principio 26 – Control y auditoría internos	El supervisor verifica que los bancos cuentan con adecuados controles internos para establecer y mantener un entorno operativo correctamente controlado que facilite la gestión de su negocio, teniendo en cuenta su perfil de riesgo. Dichos controles incluyen procedimientos claros sobre delegación de autoridad y atribuciones; separación de las funciones que implican compromisos del banco, desembolso de sus fondos y contabilidad de sus activos y pasivos; conciliación de estos procesos; protección de los activos del banco; y funciones independientes de auditoría interna y de cumplimiento para verificar la observancia de estos controles, así como de la legislación y regulación aplicables.
Principio 27 – Información financiera y auditoría	El supervisor verifica que los bancos y grupos bancarios mantienen registros adecuados y fiables, elaboran estados financieros conforme a las políticas y prácticas contables

externa	ampliamente aceptadas a escala internacional y publican anualmente información que refleja razonablemente su situación financiera y resultados y está sujeta a la opinión de un auditor externo independiente. El supervisor también verifica que los bancos y las sociedades matrices de los grupos bancarios cuentan con adecuados sistemas de buen gobierno y vigilancia de la función de auditoría externa.
Principio 28 – Divulgación y transparencia	El supervisor verifica que los bancos y grupos bancarios publican regularmente información en base consolidada y, cuando corresponda, a título individual que resulta de fácil acceso y refleja razonablemente su situación financiera, resultados, exposiciones al riesgo, estrategias de gestión del riesgo y políticas y procesos de gobierno corporativo.
Principio 29 – Utilización abusiva de servicios financieros	El supervisor verifica que los bancos cuentan con políticas y procesos adecuados, incluidas estrictas reglas de diligencia debida con la clientela, para promover normas éticas y profesionales de alto nivel en el sector financiero e impedir que el banco sea utilizado, intencionalmente o no, con fines delictivos.

Fuente: (Basilea)

Elaborado por: Elisa Sarango

2.2 Normas y mejores prácticas de organismos nacionales.

2.2.1 Superintendencia de bancos.

La Superintendencia de Bancos es un organismo de control financiero cuya finalidad es:

"La vigilancia, auditoría, intervención, control y supervisión de las actividades financieras que ejercen las entidades públicas y privadas del Sistema Financiero Nacional, con el propósito de que estas actividades se sujeten al ordenamiento jurídico y atiendan al interés general." (SIB).

La Junta Bancaria que en el código monetario aprobado el 2014 se denominará Junta de Política y Regulación Monetaria y Financiera, tiene como atribuciones entre otras las siguientes:

El Formular la política de control y supervisión del sistema financiero, aprobar las modificaciones del nivel requerido de patrimonio técnico y las ponderaciones de los activos de riesgo y pronunciarse sobre el establecimiento y liquidación de las instituciones financieras, así como de la remoción de sus administradores, así como resolver los casos no consultados en la ley, así como las dudas en cuanto al carácter bancario y financiero de las operaciones y actividades que realicen las instituciones financieras y dictar las resoluciones de carácter general relacionadas con las normas de solvencia y prudencia requeridas para la adecuada supervisión y control del sector financiero.

En su momento la Junta de Política y Regulación Monetaria y Financiera el 26 de Abril del 2012 solicito la publicación en registro oficial de la resolución JB-2012-2148 que entre otros temas incluye lineamientos de seguridad en los canales electrónicos que deben ser aplicados por las Instituciones Financieras bajo control de la Superintendencia de Bancos.

Se establecen lineamientos generales de seguridad para canales, así como lineamientos específicos por cada tipo de canal en donde el plazo final de cumplimiento es 36 meses a partir de la fecha de registro, sobre esto han existido algunas resoluciones que agregan o modifican a la resolución original como es el caso de la JB-2014-3066 del 2 se Septiembre del 2014.

Tabla 6: Resolución JB-2012-2148

Artículo	Detalle
4.3.8	Medidas de seguridad en canales electrónicos
	Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente
4.3.8.1	Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento

4.3.8.2	Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información
4.3.8.3	El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes
4.3.8.4	La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado
4.3.8.5	Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución
4.3.8.6	Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento
4.3.8.7	Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas

4.3.8.8	Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. /n Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el ó los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros. /n Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros.
4.3.8.9	Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a cajeros automáticos; dicha clave deberá ser diferente de aquella por la cual se accede a otros canales electrónicos
4.3.8.10	Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo
4.3.8.11	Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura

4.3.8.12	Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas
4.3.8.13	Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas
4.3.8.14	Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos
4.3.8.15	Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para operaciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales.
4.3.8.16	Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos /n Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado,

	identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses
4.3.8.17	Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (Call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana
4.3.8.18	Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (Call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales
4.3.8.19	Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante los centros de atención telefónica (Call center), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes
4.3.8.20	Las instituciones del sistema financiero deberán ofrecer a los clientes el envío en línea a través de mensajería móvil, correo electrónico u otro mecanismo, la confirmación del acceso a la banca electrónica, así como de las transacciones realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas
4.3.8.21	Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo
4.3.8.22	Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de

	tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos
4.3.8.23	Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos por la entidad
4.3.8.24	Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad
4.3.8.25	Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades
4.3.9	Cajeros automáticos
4.3.9	Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente
4.3.9.1	Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento
4.3.9.2	La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece
4.3.9.3	Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip
4.3.9.4	Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del

	sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
4.3.9.5	Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberán instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución
4.3.9.6	Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia
4.3.9.7	Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: “algo que se sabe, algo que se tiene, o algo que se es
4.3.10	Puntos de venta (POS y PIN Pad)
	Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente
4.3.10.1	Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta con la debida autorización

4.3.10.2	A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura
4.3.10.3	Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip
4.3.11	Banca electrónica
	Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente
4.3.11.1	Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes
4.3.11.2	Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional /n Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas
4.3.11.3	Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior
4.3.11.4	Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes

	accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero
4.3.11.5	Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión
4.3.11.6	Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones
4.3.11.7	Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica
4.3.11.8	La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS)
4.3.11.9	La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres
4.3.11.10	Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: “algo que se sabe, algo que se tiene, o algo que se es”, considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una operación, ser una clave de una sola vez OTP (one time password), tener controles biométricos, entre otros
4.3.11.11	En todo momento en donde se solicite el ingreso de una clave numérica, los sitios web de las entidades deben exigir el ingreso de éstas a través de teclados virtuales, las mismas que deberán estar enmascaradas
	Banca móvil

4.3.12	Las instituciones del sistema financiero que presten servicios a través de banca móvil deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8. y 4.3.11
	Sistemas de audio respuestas (IVR)
4.3.13	Las instituciones del sistema financiero que presten servicios a través de IVR deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8. y 4.3.11
	Corresponsales no bancarios
4.3.14	Las instituciones financieras controladas que presten servicios a través de corresponsales no bancarios deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8, 4.3.10 y 4.3.11

Fuente: Superintendencia de bancos y seguros

Elaborado por: Elisa Sarango

En resumen la resolución establece 50 literales que se debe cumplir en 3 años como plazo máximo.

2.2.2 Asociación de bancos.

La Asociación de Bancos es una entidad gremial sin fines de lucro constituida el 30 de marzo de 1965 cuya misión es velar por el desarrollo y buen funcionamiento del sistema bancario y de la economía nacional.

Esta asociación no ha dado lineamientos sobre el funcionamiento de los canales electrónicos lo que sí ha hecho en sus comunicaciones y boletines es emitir recomendaciones para el uso de canales electrónicos. Se encuentra vinculados a la asociación de Bancos 15 instituciones financieras del país.

CAPÍTULO III: MECANISMOS DE SEGURIDAD APLICADOS POR LA BANCA ECUATORIANA

3.1 Análisis de canales electrónicos.

Las instituciones financieras de nuestro país han ido adoptando principios de seguridad principalmente en función de lo normado por la Junta Bancaria.

Para determinar los esquemas de seguridad aplicados en los canales electrónico se aplica una encuesta a los clientes del sistema financiero. El tamaño de la muestra para la aplicación de la encuesta se lo determina de la siguiente forma:

$$n = \frac{k^2 Npq}{e^2(N-1) + k^2 pq}$$

N: Tamaño de la población o universo
k: Nivel de confianza, en este caso aplicaremos el 95% que en base a la tabla de distribución normal corresponde al 1,96.
e: Es el error muestral deseado que se considerar en este caso el 5% (0,05)
p: porción estimada de éxito.
q: porción estimada de fracaso.
En estos dos últimos al ser desconocidos se consideran 0.5
Reemplazando la formula especificada, se obtiene:

$$n = \frac{(1{,}96)^2 * 2000000 * (0{,}5) * (0{,}5)}{((0{,}05)^2 * (2000000 - 1)) + (1{,}96^2) * (0{,}5) * (0{,}5)}$$

$$n = 384$$

Grupo Objetivo: Clientes del sistema financiero en análisis que utilizan canales electrónicos.
Género: hombres y mujeres.
Edad: Mayores a 18 años.
Tamaño de muestra: 384 encuestas.
Fecha: Marzo 2015
Técnica de recolección de datos: Aplicación de encuesta online mediante sistema de formulario de Google.

La encuesta que se aplicó consta de 8 preguntas con la finalidad de conocer el uso de los canales electrónicos por parte de los clientes de las instituciones financieras y así mismo

determinar si los mecanismos de seguridad aplicados de acuerdo a la resolución han hecho más complicado el uso de los canales.

Considerando que el análisis está centrado de manera particular a tres instituciones, la primera pregunta se utiliza para clasificar a que entidad financiera pertenece la persona encuestada.

De acuerdo a la aplicación de la encuesta se obtuvieron los siguientes resultados:

3.1.1 Análisis de resultados de encuesta de canales electrónicos.

A continuación se presenta la interpretación de los resultados obtenidos de la encuesta aplicada a 318 clientes de las instituciones financieras.

Existe una diferencia entre la muestra dado por el mecanismo aplicado para la ejecución de la encuesta, al bajar el número de encuestas a 318, el error muestral tiene una variación del 5% al 5,5% lo cual sigue siendo aceptable para el análisis realizado.

Pregunta # 1: Indique de que institución financiera es cliente

Tabla 7: Pregunta #1

Respuesta	Frecuencia	Porcentaje
Banco de Loja	207	65%
Banco Pichincha	85	27%
Produbanco	26	8%
Total General	318	100%

Autor: Elisa Sarango

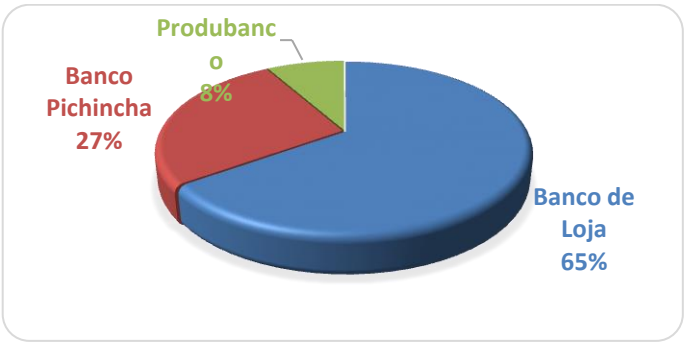


Ilustración 20: Pregunta #1
Autor: Elisa Sarango

Análisis: En base a la encuesta aplicada el 65% de los clientes indican que usan Banco de Loja, esto se debe a la distribución de la base de emails de clientes sobre la cual se aplicó la encuesta ya que de acuerdo a la información de la SIB el Banco Pichincha tiene el mayor número de clientes a nivel del país. En este caso un 27% de clientes han indicado que son clientes de Banco Pichincha y un 8% Produbanco.

Pregunta # 2: Utiliza usted los canales electrónicos de su Banco.

Tabla 8 : Pregunta #2

Respuesta	Frecuencia	Porcentaje
SI	318	100%
NO	0	0%
Total General	318	100%

Autor: Elisa Sarango

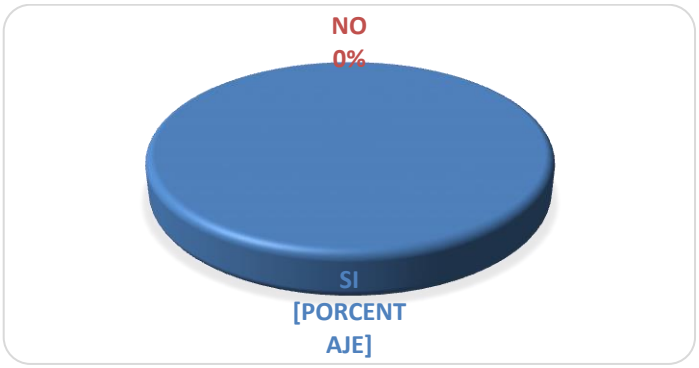


Ilustración 21: Pregunta #2
Autor: Elisa Sarango

Análisis: La totalidad de los clientes encuestados indican que utilizan canal electrónico, esto es al menos alguno de los canales disponibles en su Banco, aquí cabe recalcar que esto se produce ya que las encuestas se dirigieron de manera electrónica y los usuarios de Internet tienen mayor tendencia al uso de canales electrónicos por los conocimientos que dispone de la red.

Pregunta # 3: ¿Cuál de los siguientes canales electrónicos utiliza?

Tabla 9 : Pregunta #3

Respuesta	Frecuencia	Porcentaje

Banca Electrónica	203	64%
Cajero Automático	300	94%
Banca Móvil	7	2%
Telemático	2	1%

Autor: Elisa Sarango

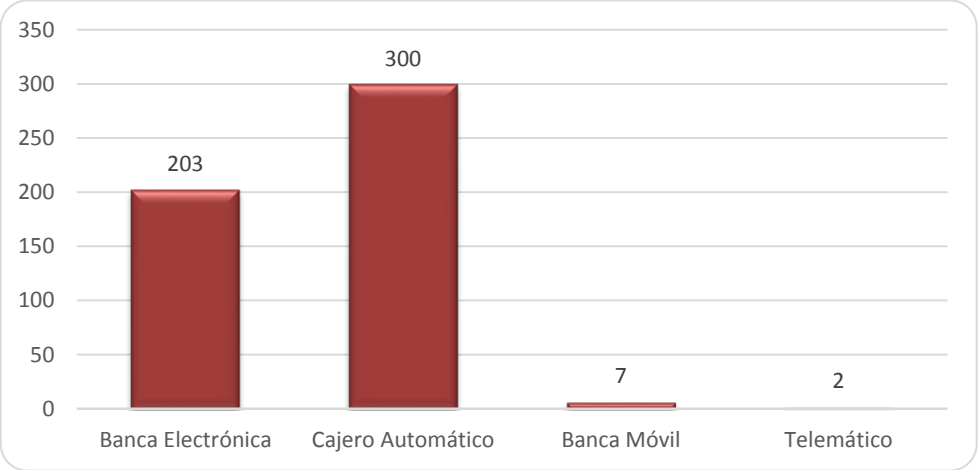


Ilustración 22 : Pregunta #3

Autor: Elisa Sarango

Análisis: El canal con mayor porcentaje de uso en los clientes es el cajero automático con un 94% de uso, por lo que las instituciones financieras deben prestar mucha atención sobre las seguridades, así mismo el otro canal que tiene un alto porcentaje de uso en los clientes es la Banca Electrónica.

Pregunta # 4: ¿Considera usted que los canales electrónicos son seguros?

Tabla 10: Pregunta #4

Respuesta	Frecuencia	Porcentaje
SI	232	73%
NO	86	27%
Total general	318	100%

Autor: Elisa Sarango

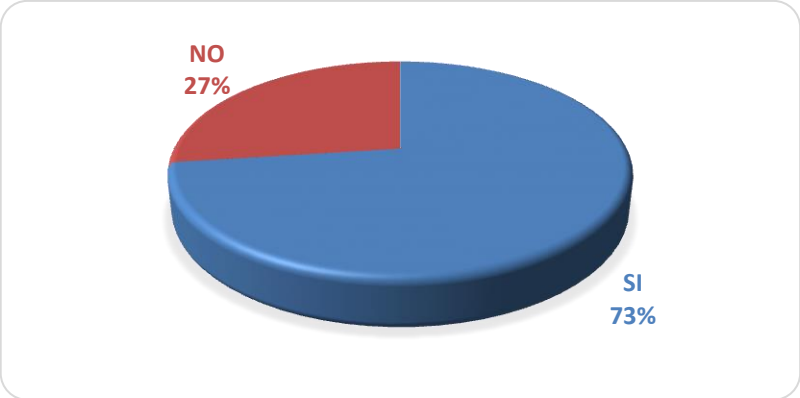


Ilustración 23 : Pregunta #4

Autor: Elisa Sarango

Análisis Un 27% de los clientes consideran que los canales electrónicos no son seguros, esto puede deberse a varios factores como haber sido víctima de fraude electrónico, desconocimiento de Internet, falta de conocimientos del uso del computador, los cual puede generar que no se utilicen los canales electrónicos.

Pregunta # 5: ¿Los canales electrónicos de su Banco son fáciles de utilizar?

Tabla 11 : Pregunta #5

Respuesta	Frecuencia	Porcentaje
SI	318	100%
NO	0	0%
Total General	318	100%

Autor: Elisa Sarango

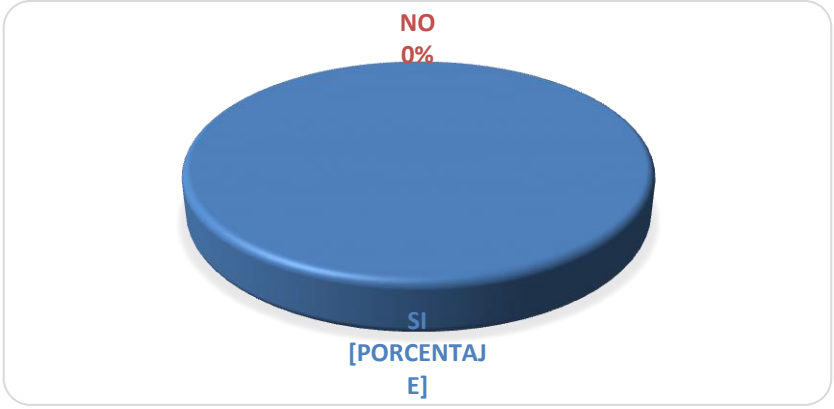


Ilustración 24 : Pregunta #5

Autor: Elisa Sarango

Análisis*:* La totalidad de clientes encuestados indican que los canales son sencillos de utilizar, lo cual indica que las seguridades que se han colocado no han afectado el grado de usabilidad de los mismos.

Pregunta # 6: *¿Ha sido víctima de un fraude en canal electrónico?*

Tabla 12 : Pregunta #6

Respuesta	Frecuencia	Porcentaje
NO	305	96%
SI	13	4%
Total general	318	100%

Autor: Elisa Sarango

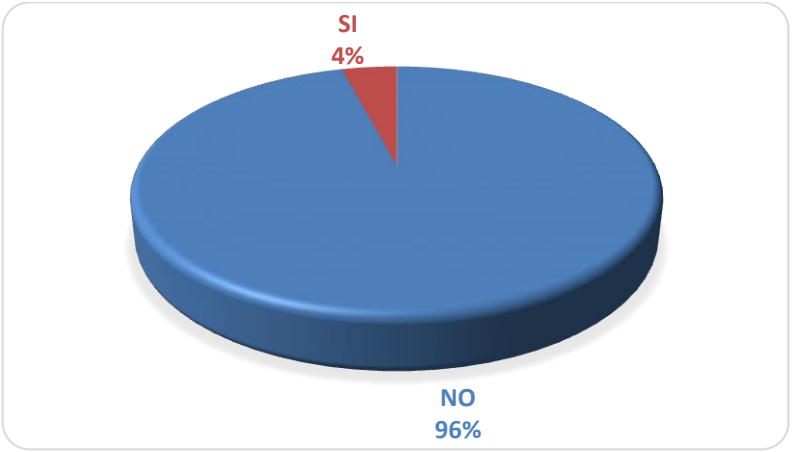


Ilustración 25 : Pregunta #6

Autor: Elisa Sarango

Análisis: Un 4% de los clientes indican que han sido víctimas de algún tipo de fraude en canal electrónico, los fraudes en canales electrónicos son más comunes en instituciones con mayor número de usuarios.

Dentro de los principales fraudes que se han producido estos se deben principalmente a clonación de tarjetas de débito las cuales normalmente son cubiertos por los Bancos dado que la clonación se produce por falta de seguridades en los cajeros automáticos, el otro caso de fraude es compras en POS mediante débito para lo cual se utiliza también la tarjeta de débito y en estos casos lo más común es que los comercios no solicitan la identificación del cliente con los cual una tarjeta robada, en estos casos el Banco debe pagar por el fraude y escalar el problema al comercio.

3.1.2 Análisis de canales electrónicos en los bancos investigados.

Para el presente trabajo de investigación, se consideraron como sectores estratégicos para la recolección de información tres de los bancos privados de Loja como son Banco Pichincha, Banco de Loja y Produbanco.

De acuerdo a los tipos de canales descritos en el capítulo I se realizaron los análisis para obtener los mecanismos de seguridad aplicados por cada uno de ellos.

En primer lugar se inicia con el análisis de la institución financiera Banco de Loja, la cual dispone de canales electrónicos para sus clientes y cuenta con los siguientes tipos de seguridad por cada uno de ellos:

Banco de Loja.

De acuerdo a la memoria institucional del Banco de Loja y a las consultas realizadas a los administradores de los canales a continuación se indican los canales electrónicos y sus mecanismos de seguridad.

Banca Telefónica: Este servicio cuyo nombre comercial es Loja Alo dispone a los clientes de un mecanismo para realizar transacciones de consulta, es decir no existen transacciones que impliquen movimiento de dinero, para acceder a este canal se utilizan la cedula de identidad y una contraseña asignada por la institución con lo cual se permite el acceso.

El mecanismo de seguridad aplicado en este canal es el uso de una contraseña, no existe otro mecanismo de seguridad visible para el cliente, hay que considerar que existen mecanismos de para obtener información que viaje en el canal telefónico por lo que existe la vulnerabilidad de obtener los datos que viajan por este canal pero al ser únicamente de consultas y emergencia bancarias no existe un riesgo de pérdida económica.

Cajeros automáticos: Banco de Loja cuenta con aproximadamente 40 cajeros, los cuales permiten realizar retiros de dinero y transferencias entre cuentas propias. Para el funcionamiento del cajero el cliente recibe una tarjeta de débito al momento con Banda Magnética la cual es muy fácil de clonar y una clave para el acceso al canal, estos cajeros permiten procesamiento con chip sin embargo los clientes aun no cuentan con tarjeta con chip, el chip es un dispositivo que viene en la tarjeta y que a la fecha no existen reportes de

clonación, adicionalmente estos cajero cuentan con varillas en las lectoras que impiden que se coloquen objetos extraños para realizar clonaciones, el número de transacciones realizadas por este canal es de 200.000 transacciones mensuales de acuerdo a los datos publicados por esta institución en su memoria institucional del año 2013 (B.L. Memoria)

Banca electrónica: Este canal dispone de opciones para transferencia de dinero a cuentas del mismo banco y de otros bancos, pago de servicios básicos, recargas de servicios, opciones de consulta, los clientes para utilizar este canal tienen un acceso mediante el uso de usuario, contraseña, ingreso de una imagen y contestación de pregunta, para realizar transacciones que impliquen movimiento de dinero deben disponer de una tarjeta de coordenadas entregada por la institución con lo cual se minimiza el riesgo de fraude, en esta institución no se ha evidenciado casos de intento de clonación del sitio web, adicionalmente utiliza un certificado de seguridad para la veracidad del sitio, se realizan en promedio 250.000 transacciones mensuales por este canal de acuerdo a (B.L. Memoria).

Banco Pichincha

Banca telefónica: El servicio ofrecido por la institución permite realizar transacciones de consulta y movimiento de dinero, para acceder al mismo el cliente requiere del ingreso de su número de cedula y una clave de acceso proporcionada por el banco para poder realizar las transacciones de movimiento de dinero es necesario que el cliente disponga de una tarjeta de coordenadas.

Cajeros automáticos: Banco Pichincha dispone de aproximadamente 830 cajeros automáticos, los cuales permiten realiza transacciones de retiro de dinero, transferencia, pagos de servicios, recarga de servicios. Para el uso de este canal el cliente requiere de una tarjeta de débito la cual al momento esta institución la proporciona con chip y se encuentra en proceso de migración a sus clientes, al no estar todas las instituciones financieras migradas a un esquema de chip es posible aun la clonación de estas tarjetas, así mismo los cajeros están siendo reemplazados para soportar procesamiento con chip, esta red de cajero aún no está al 100% migrada a esta nueva tecnología. Este canal realiza 6,61 millones de transacciones por mes, moviendo montos de 79 millones de dólares anuales, esta información ha sido tomada de la memoria institucional de esta entidad año 2013 (B. P. Memoria).

Banca electrónica: El cliente para acceder a este canal utiliza un usuario y contraseña, este canal dispone de un sistema biométrico que detecta el ritmo de digitación de la contraseña y si el cliente la digita con otro patrón le solicita el ingreso de un código de uso único enviado al celular o correo electrónico, este canal así mismo dispone de un certificado digital para el cifrado de la información, para realizar transacciones el cliente requiere del uso de una tarjeta de coordenadas, sin esta tarjeta no se pueden realizar transacciones de movimiento de dinero. Por este canal se realizan 11.000.000 de transacciones anuales de acuerdo a (B. P. Memoria).

Produbanco

Banca telefónica: El servicio ofrecido por Produbanco tiene las mismas características y seguridades del canal del Banco Pichincha.

Cajeros automáticos: Produbanco dispone de aproximadamente 200 cajeros automáticos, los cuales permiten realiza transacciones de retiro de dinero, transferencia, pagos de servicios, recarga de servicios. Para el uso de este canal el cliente requiere de una tarjeta de débito la cual ya dispone de chip, no se han encontrado datos en relación a la transaccionalidad de este canal

Banca electrónica: El cliente para acceder a este canal utiliza un usuario y contraseña, se solicita responde a una pregunta de verificación, este canal así mismo dispone de un certificado digital para el cifrado de la información, para realizar transacciones el cliente requiere del uso de una tarjeta de coordenadas, sin esta tarjeta no se pueden realizar transacciones de movimiento de dinero.

3.1.3 Análisis de canales electrónicos en cooperativas.

Las cooperativas en nuestro país en su mayoría disponen únicamente de cajeros automáticos como canales electrónicos, al momento las cooperativas disponen de transacciones de retiros y transferencias en los cajeros y para el uso del mismo se lo hace por medio de una tarjeta de débito y una clave de acceso, la mayor parte están ejecutando los proyectos para cumplir la normativa, sin embargo esto puede tomar todo el 2015 para ser completado.

3.2 Esquemas de cambio de responsabilidad para cobertura de fraudes.

Se ha implementado por parte de Banred[11] esquemas de cambio de responsabilidad, es decir que la entidad que no cumple con implementación de chip debe pagar por los fraudes que se produzcan en sus cajeros o tarjetas que no procesen chip. Este esquema ha sido aplicado por Banred para todos los bancos que están incluidos en la red.

Para el procesamiento de transacciones normalmente hay al menos tres actores que intervienen, uno actor corresponde al Emisor que es el banco que entrega la tarjeta al cliente, el adquiriente es el banco en donde se está realizando la transacción y el integrador en este caso es Banred.

El mecanismo de cambio de responsabilidad es el esquema para determinar qué entidad de pagar por el fraude realizado en la transacción de cajero automático y funciona de la siguiente manera:

- Si el adquiriente de la transacción permite mediante sus cajeros el procesamiento de chip y el emisor aun no entrega tarjetas con chip este último es el responsable de pagar por el fraude.
- Si el cliente del emisor dispone de tarjeta con chip y el adquiriente no tiene preparado sus cajeros para soportar chip este último debe responde ante un fraude producido en estas condiciones.
- Si tanto emisor como adquiriente procesa chip, el emisor responde por los fraudes, según la tecnología chip estos casos no deberían darse.

Esto forzar a las instituciones a cuidar sus esquemas de seguridad con la finalidad de minimizar el número de fraudes por este medios.

En los otros canales la responsabilidad es directa de la institución que ofrece el servicio, hay que entender que muchos fraudes se producen por la cultura financiera y tecnológica de los clientes.

[11] Banred: Institución que integra la una red de cajeros automáticos

3.3 Mecanismos de atención de reclamos por fraudes.

Todas las instituciones financieras están obligadas a mantener una unidad de atención al cliente en donde se deben receptar los reclamos de los clientes los cuales deben ser atendidos en máximo 15 días, si no es atendido durante ese periodo de tiempo es posible canalizar un reclamo mediante la SIB siempre cuando se haya agotado la primera instancia y esto tiene que evidenciarse ante la SIB, dichos reclamos corresponde a cualquier queja que se realicen por parte del cliente sean estos por de afectación monetaria o por temas propios de servicio en la institución.

Así mismo según lo dispuesto en el tercer inciso del artículo 312 de la Constitución de la República del Ecuador establece que cada entidad integrante del sistema financiero nacional tendrá una defensora o defensor del cliente, que será independiente de la institución y designado de acuerdo a la ley.

En la resolución JB-2012-2226 de 10 de julio de 2012, se han reglamentado las funciones, alcance, competencias, obligaciones y prohibiciones del Defensor del Cliente, así como el procedimiento que llevará a cabo para la atención de reclamos.

En el *Art. 5, Capítulo V, del Título XIV, Libro I de la Codificación de Resoluciones de la SIB Y JB se indica la función del defensor del cliente:*

"La o el defensor del cliente tiene como función proteger los derechos e intereses particulares de los clientes de la respectiva institución del sistema financiero, para lo cual conocerá y tramitará los reclamos sobre todo tipo de negocios financieros que tengan relación directa con el cliente reclamante, a cuyo efecto recabará de éste la autorización expresa que le faculte a solicitar información o documentación a la institución del sistema financiero, relacionada con el reclamo."

CAPÍTULO IV: ANÁLISIS DE LOS FRAUDES ELECTRÓNICOS Y CUMPLIMIENTO DE LAS NORMATIVAS NACIONALES E INTERNACIONALES

4.1 Impacto Económico de los fraudes en canales electrónicos.

Los fraudes en canales electrónicos implican perdidas económicas sean estas para el cliente como para la institución financiera, no existe información consolidada en relación a esta pérdidas, por lo que se ha tomado las memorias institucionales de los Bancos en análisis, sin embargo el único Banco que tiene publicada su información cuantificada es Pichincha en el cual se indica que en el 2012 los fraudes ascendieron a 8'876.212,98 disminuyendo estos en el 2013 a 4'608.227,86.

4.2 Cumplimiento de la resolución JB-2012-2148.

Se realizará el análisis del cumplimiento de cada uno de los puntos de la resolución 2148 en cada una de las instituciones alcance del presente trabajo, los puntos del artículo 4.3.8 corresponden a puntos generales aplicables en todos los canales de las instituciones y la aplicación de estos no son visibles para los clientes ya que son herramientas y políticas internas, se describe la forma de cumplimiento por cada uno de los puntos de la norma. Cabe indicar que en los casos en donde el cumplimiento es genérico en todas las instituciones se describe como una sola solución y en los casos en donde hay variación se describe la solución por cada institución analizada.

"4.3.8.1 Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento"

Forma de cumplimiento: Implementación de procedimientos internos.

"4.3.8.2 Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información"

Forma de cumplimiento: Implementación de procedimientos internos.

"4.3.8.3 El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes".

Forma de cumplimiento: Instalación de herramienta de cifrado de correo electrónico la cual permite detectar que se está enviando información como números de cuentas, tarjetas y lo que hace es cifrar esta información mediante un correo seguro.

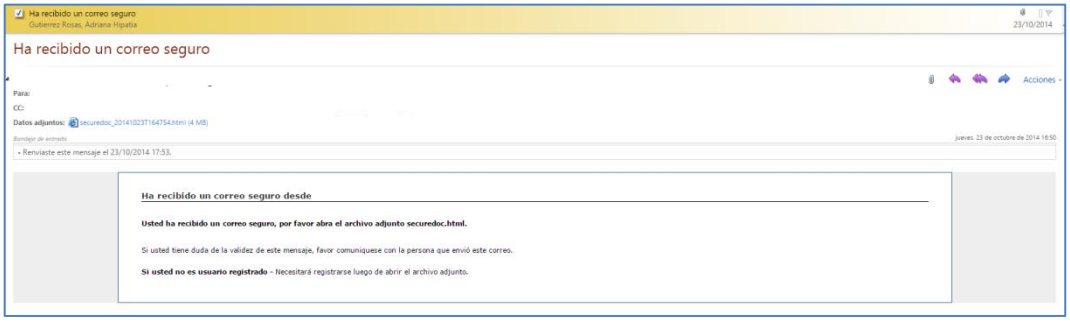


Ilustración 26: Correo seguro

Fuente: Banco de Loja

"4.3.8.4 La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado"

Forma de cumplimiento: Implementación de mecanismo de encriptación de los enlaces de comunicación.

"4.3.8.5 Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución"

Forma de cumplimiento: Instalación de herramienta antimalware en los servidores que alojan los canales electrónicos, estos permiten detectar si se instalan programas no autorizados.

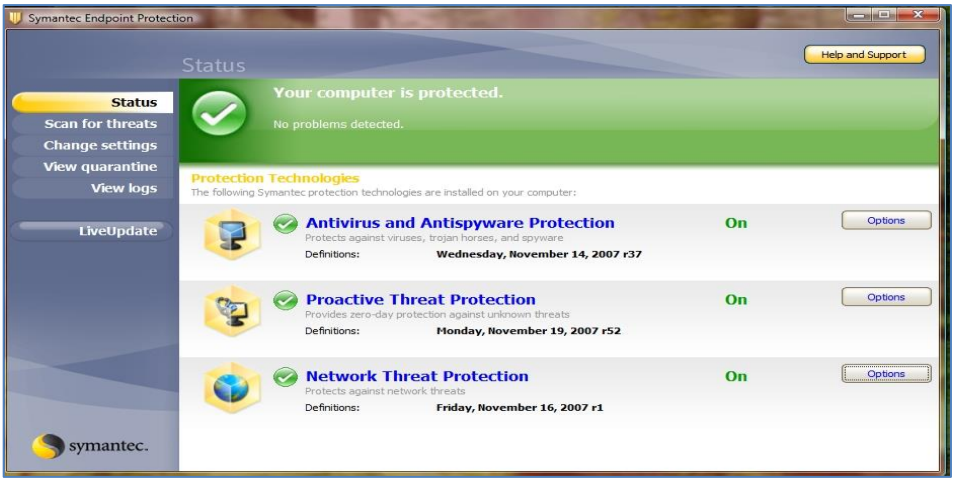


Ilustración 27: Antimalware

Fuente: http://en.wikipedia.org/wiki/Symantec_Endpoint_Protection

"4.3.8.6 Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento"

Forma de cumplimiento: Implementación de equipos específicos para almacenamiento de claves (caja atalla)

Ilustración 28: Caja atalla

Fuente: www8.hp.com/cl/es/software-solutions/data-security-encryption/

"4.3.8.7 Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas."

Forma de cumplimiento: El funcionamiento de los canales depende de muchos factores como son redes de comunicación, servidores de aplicaciones, bases de datos, el propio canal entre otros factores, por lo que para poder cumplir este punto se han implementado mecanismos de monitoreo en cada uno de los puntos de posible compromiso, este monitoreo alerta mediante sms, llamada telefónica y correo electrónico al responsable del canal sobre la novedad presentada.

".3.8.8 Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. /n Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el o los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros. /n Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros."

Forma de cumplimiento: Para cubrir lo que corresponde al canal electrónico han implementado mecanismos para que el cliente pueda personalizar sus valores de transacción mediante canal físico o electrónico el valor está en función de los montos máximos establecidos por cada institución.

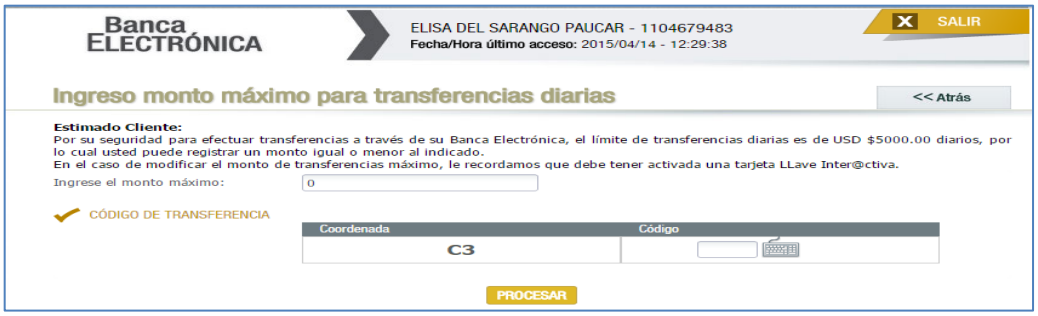


Ilustración 29: Personalización de montos de transferencia

Fuente: Banco de Loja

Para el cumplimiento a nivel de tarjetas de crédito o débito existe un solo cupo asignado en la misma y no se puede separar monto por consumos nacionales o internacionales, razón por la cual la personalización consiste en activar o bloquear el consumo nacional e internacional.

Ilustración 30: Personalización de redes de consumo

Fuente: www.interdin.com.ec

"4.3.8.9 Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a cajeros automáticos; dicha clave deberá ser diferente de aquella por la cual se accede a otros canales electrónicos."

Forma de cumplimiento: En este caso se indica que se debe modificar los procedimientos, sin embargo aquí existen ajustes a nivel de las plataformas de los canales de tal manera que se solicite el cambio de contraseña al año de haberla registrado, esto ocasiona inconvenientes y muchos bloqueos de los canales ya que los usuarios al cambiarla no la recuerdan.

"4.3.8.10 Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo"

Forma de cumplimiento: Se han implementado herramientas de inteligencia artificial que permitan aprender del comportamiento del cliente con la finalidad de alerta cuando existe un comportamiento fuera de sus costumbres, en el canal Banca Electrónica, Móvil, Telemático es posible alertar de manera oportuna para bloquear la transacción, en el caso de tarjetas no es posible dado que la transacción es directa por lo que en este caso se han implementado mecanismos de bloqueo posteriores a la transacción.

“4.3.8.11 Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura.”

Forma de cumplimiento: Se realiza el bloqueo del canal al tercer intento erróneo y se envía un mail y/o SMS indicando este bloqueo.

“4.3.8.12 Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos.”

Forma de cumplimiento: Esto se ha implementado a nivel de responsabilidades internas en los manuales de procedimientos.

4.3.8.13 Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas.

Forma de cumplimiento: Esto se ha implementado a nivel de responsabilidades internas en los manuales de procedimientos.

“4.3.8.14 Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos”

Forma de cumplimiento: Se han implementado servidores de tiempo con la finalidad de que todos los canales estén integrados para tomar la fecha y hora del servidor principal, de esta manera se evita que exista transacciones con un registro en los logs del canal y otro registro en las bases de datos.

“4.3.8.15 Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de

transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para operaciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales."

Forma de cumplimiento: En este punto antes de ser emitida la norma los Bancos ya disponían de esta información en sus canales, razón por la cual no existió un esfuerzo adicional para la implementación.

"4.3.8.16 Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos /n Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses"

Forma de cumplimiento: Para efectos de hacer desarrollo de sus aplicativos las instituciones del sistema financiero utilizan ambientes de pruebas en donde normalmente suben respaldo de la información real, para cumplir con este punto se identificó por parte de las instituciones la información que deben cifrar de tal manera que los ambientes tengan información no legible para quienes la consulten.

"4.3.8.17 Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (Call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana."

Forma de cumplimiento: Para el cumplimiento de las emergencias bancarias y con la finalidad de evitar tener personal 24x7 se han implementado sistemas automático que permiten al cliente atender requerimientos de bloqueos, perdidas, robos, activaciones considerados como emergencias bancarias.

“4.3.8.18 Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (Call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales.”

Forma de cumplimiento: Las herramientas para call center realizan la grabación de las llamadas, las llamadas que las instituciones no graban son las que se realizan directamente a los oficiales, ya que no se tiene un esquema de control para evidenciar que tipo de servicio están brindando a los clientes por lo que deberían grabarse todas las llamadas.

“4.3.8.19 Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante los centros de atención telefónica (Call center), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes.”

Forma de cumplimiento: Este aspecto no lo cumplen las instituciones financieras dado que para realizar una llamada se utilizar el canal de comunicación de telefonía pública o privada sobre el cual no tienen controla las IFIS.

“4.3.8.20 Las instituciones del sistema financiero deberán ofrecer a los clientes el envío en línea a través de mensajería móvil, correo electrónico u otro mecanismo, la confirmación del acceso a la banca electrónica, así como de las transacciones realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas.”

Forma de cumplimiento: Las instituciones están enviando las notificaciones en los eventos indicados en este punto principalmente por correo electrónico y SMS están haciéndolo discrecionalmente principalmente por el costo en el cual incurren por este envío.

“4.3.8.21 Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo.”

Forma de cumplimiento: En el caso de Banco Pichincha y Produbanco se encuentra implementado, en Banco de Loja se ha implementado la tarjeta de crédito y están en proceso de implementación de la tarjeta de débito.

"4.3.8.22 Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos"

Forma de cumplimiento: Las instituciones están capacitando mediante emailing, sus páginas web, y en los canales con información en relación a las medidas de seguridad.

"4.3.8.23 Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos por la entidad."

Forma de cumplimiento: Se está informando al cliente mediante su página web, pero no existe una evidencia en sí de capacitación implícita del tema.

"4.3.8.24 Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad."

Forma de cumplimiento: Los planes anuales de auditoría incluyen la verificación del cumplimiento de la normativa.

"4.3.8.25 Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades"

Forma de cumplimiento: Se han establecido procedimiento para implementación de código seguro.

“4.3.9.1 Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento”

Forma de cumplimiento: En el momento en que el cliente ingresa la contraseña esta se cifra, adicionalmente el canal de comunicación de los cajeros tiene mecanismos de cifrado.

“4.3.9.2 La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece”

Forma de cumplimiento: Se han instalado software de control que permite que cuando se conecta un dispositivo desconocido este no es reconocido como parte del sistema y no se permite realizar ninguna acción.

“4.3.9.3 Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip”

Forma de cumplimiento: Las instituciones han realizado los desarrollos de software a nivel de los cajeros para soportar las tramas de mensajería chip, así mismo han realizado los cambios de hardware para permitir la lectura de las tarjetas con chip, cuando se realiza una transacción con chip la tarjeta es retenida en la lectora durante toda la transacción y cuando es con banda la tarjeta debe ser insertada y retirada inmediatamente.

“4.3.9.4 Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores”

Forma de cumplimiento: Todos los cajeros vienen con las especificaciones técnicas de instalación y las instituciones financieras realizan la instalación de acuerdo a esto ya que de esta forma pueden mantener las garantías de sus proveedores.

“4.3.9.5 Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así

mismo, se deberán instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución"

Forma de cumplimiento: Las instituciones han implementado software de fabricantes como Symantec, McAfee para dar cumplimiento a este punto.

"4.3.9.6 Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia"

Forma de cumplimiento: El plan de auditoria de las instituciones financieras incluye el análisis de las seguridades de los cajeros automáticos.

"4.3.9.7 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es"

Forma de cumplimiento: Para esto en el caso de Banco de Loja se ha implementado el acceso con usuario, contraseña, pregunta y en la ejecución de transacciones se utiliza la tarjeta de coordenadas.

Puntos de venta (POS y PIN Pad)

"4.3.10.1 Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta con la debida autorización"

Forma de cumplimiento: Esto es procedimental, dado que el comercio lo debe asegurar para permitir el acceso solo a personal que se identifique con las credencias

proporcionadas, por otro lado las instituciones financieras notifican previamente la asistencia del técnico enviando un correo con la fotografía del personal.

"4.3.10.2 A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura".

Forma de cumplimiento: Se está realizando el proceso de migración de los POS en los establecimientos para permitir la conexión inalámbrica.

"4.3.10.3 Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip"

Forma de cumplimiento: Se está realizando el reemplazo de los equipos para colocar dispositivos que soporten el procesamiento de chip.

Ilustración 31: Punto de venta

Fuente: http://www.canstockphoto.com/images-photos/pin-pad.html

Banca electrónica.

"4.3.11.1 Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes"

Forma de cumplimiento: Es aspecto se ha cumplido con la implementación de certificados de seguridad, esto se evidencia cuando la conexión al inicio de la dirección web inicia con

https, en donde la “s” indica que es seguro el acceso, adicionalmente en el caso de Banco de Loja, y Pichincha se tiene un certificado de barra verde el cual da aun mayor seguridad para el cliente.

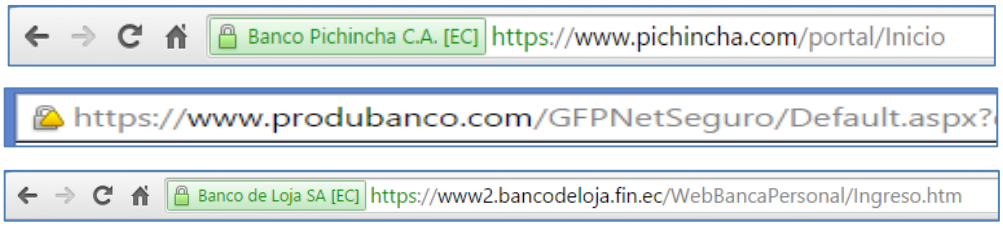


Ilustración 32: Certificado digital

Fuente: Sitios web de Instituciones financieras.

“4.3.11.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional /n Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas”

Forma de cumplimiento: Las instituciones financieras realizan anualmente contrataciones con proveedores para realizar Ethical hacking con la finalidad de identificar vulnerabilidades en los canales y red interna, producto de esto se realiza un plan de trabajo para ajustar las novedades presentadas.

“4.3.11.3 Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior”

Forma de cumplimiento: Los informes de los análisis se reportan a las SIB para la gestión que corresponda.

“4.3.11.4 Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero”

Forma de cumplimiento: Las instituciones han contratado servicios que se encarga de scanear sitios en la red buscando páginas similares clonadas con la finalidad de reportarlas y bloquearlas.

"4.3.11.5 Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión"

Forma de cumplimiento: El IDS es un sistema de detección de intruso, el IPS un sistema de prevención de intrusos, y los firewalls son mecanismos que permiten bloquear preventivamente puertos de acceso y dar accesos solo equipos autorizados.

"4.3.11.6 Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones"

Forma de cumplimiento: Las Bancas electrónicas luego de un tiempo de inactividad normalmente 5 minutos se cierra y requiere que el cliente se vuelva a autenticar con la finalidad de evitar que una persona no autorizada use la banca de alguien que olvido dejar cerrando la página.

"4.3.11.7 Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica"
Forma de cumplimiento: Los canales de las instituciones informan al cliente cada inicio de sesión. En el caso de Banco Pichincha lo hace mediante el envío de un código de autorización para el acceso.

Ilustración 33: Información de último acceso

Fuente: Banco de Loja

"4.3.11.8 La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS)"

Forma de cumplimiento: Se ha implementado la solución del punto 4.3.11.4.

"4.3.11.9 La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres"

Forma de cumplimiento: Se realizó la migración de los mecanismos de acceso ya que las instituciones por facilidad para los clientes utilizaban el número de identificación, al momento las instituciones han migrado el esquema de acceso para cumplir la normativa.

"4.3.11.10 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es", considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una operación, ser una clave de una sola vez OTP (one time password), tener controles biométricos, entre otros"

Forma de cumplimiento: Para dar cumplimiento a este punto se han implementado los siguientes esquemas:

Banco de Loja y Produbanco utiliza tarjeta de coordenadas, este esquemas es más vulnerable si alguien roba la tarjeta al cliente.

Banco Pichincha realizo el cambio de este esquema de tarjetas de coordenadas a OTP el cual es un password de uso único que se envía al cliente a su celular o email el momento que requiere realizar la transacción, tiene una duración de 5 minutos y solo se puede usar en una sola transacción.

"4.3.11.11 En todo momento en donde se solicite el ingreso de una clave numérica, los sitios web de las entidades deben exigir el ingreso de éstas a través de teclados virtuales, las mismas que deberán estar enmascaradas"

Forma de cumplimiento: En el caso de Produbanco se aplicó el esquema para clave numérica o alfanumérica.

Ilustración 34: Teclado para ingreso de clave

Fuente: Produbanco

En el caso de Banco de Loja y Banco Pichincha se utiliza en los casos de ingreso de clave numérica.

Este mecanismo se implementa con la finalidad de que no se puedan capturar las pulsaciones de las teclas con aplicativos llamados keylogger.

4.3 Cumplimiento de los lineamientos de la basilea.

A continuación se presenta el análisis del cumplimiento de los principios para una supervisión eficaz de acuerdo a la Basilea.

Nombre	Cumplimiento
Principio 1 – Atribuciones, objetivos y potestades	Se cumple completamente, de acuerdo al Código Orgánico Monetario y financiero, en la sección 3, artículos 60,62 y 63 los organismos de control tienen la potestad de autorizar a los Banco, realizar supervisión continua y adoptar medidas correctivas.
Principio 2 – Independencia, rendición de cuentas, recursos y protección legal de los supervisores	Se cumple completamente, el organismo de control tiene independencia, y de acuerdo al código monetario sección 3 artículo 70 este organismo debe realizar rendición de cuentas.
Principio 3 – Cooperación y colaboración	En este caso se puede decir que se cumple, sin embargo existen esquemas internacionales como la ley FATCA en la cual deben participar algunas instituciones financieras del país en la cual deben compartir cierta información de los clientes a EEUU.

Principio 4 – Actividades permitidas	Se cumple completamente.
Principio 5 – Criterios para la concesión de licencias	Se cumple completamente.
Principio 6 – Cambio de titularidad de participaciones significativas	Se cumple completamente.
Principio 7 – Adquisiciones sustanciales	Se cumple completamente.
Principio 8 – Enfoque supervisor	Se cumple completamente.
Principio 9 – Técnicas y herramientas de supervisión	Se cumple completamente.
Principio 10 – Informes de supervisión	Se cumple completamente.
Principio 11 – Potestades correctivas y sancionadoras del supervisor	Se cumple completamente.
Principio 12 – Supervisión consolidada	Se cumple completamente.
Principio 13 – Relaciones entre el supervisor de origen y el de destino	Se cumple completamente.
Principio 14 – Gobierno corporativo	Se cumple completamente. Se emitió la regulación resol_JB-2013-2392 que incluye los lineamientos del buen gobierno corporativo
Principio 15 – Proceso de gestión del riesgo	Se cumple completamente, y al momento se está aplicando la auditoria GREC en todas las instituciones financieras el cual es una metodología integral que abarca G: Gobierno Corporativo, R:Evaluacion de riesgos, E: Evaluación económica-financiera, C: Nivel de cumplimiento de normativas
Principio 16 – Suficiencia de capital	Se cumple completamente, el organismo de control existe requerimiento de capital, provisiones, entre otros
Principio 17 – Riesgo de crédito	Se cumple completamente

Principio 18 – Activos dudosos, provisiones y reservas	Se cumple completamente, el organismo de control exige provisiones de acuerdo a la calificación de la cartera
Principio 19 – Concentración de riesgos y límites de exposición a grandes riesgos	Se cumple completamente, los Bancos están obligados a mantener políticas y procesos claros, de hecho en las instituciones existe en su estructura un departamento de procesos que cumple parte de estas funciones
Principio 20 – Transacciones con partes vinculadas	Se cumple completamente, están prohibidas las transacciones vinculadas en las instituciones financieras.
Principio 21 – Riesgo país y riesgo de transferencia	Se cumple parcialmente, no existe un lineamiento claro para este punto
Principio 22 – Riesgo de mercado	Se cumple completamente y está a cargo de las unidades de riesgo de las IFIS, existen estructuras que se reportan mensualmente a la SIB.
Principio 23 – Riesgo de tasa de interés en la cartera de inversión	Se cumple completamente y está a cargo de las unidades de riesgo de las IFIS, existen estructuras que se reportan mensualmente a la SIB.
Principio 24 – Riesgo de liquidez	Se cumple completamente y está a cargo de las unidades de riesgo de las IFIS, existen estructuras que se reportan mensualmente a la SIB
Principio 25 – Riesgo operacional	Se cumple completamente, el organismo de control está monitoreando constantemente el cumplimiento de las políticas de riesgo operativo.
Principio 26 – Control y auditoría internos	Se cumple completamente, existe procesos de auditoria interna, externa y del organismo de control
Principio 27 – Información financiera y auditoría externa	Se cumple completamente, existe procesos de auditoria interna, externa y del organismo de control
Principio 28 – Divulgación y transparencia	Se cumple completamente, todas las instituciones están obligadas a publicar la información en espacios de transparencia como sitios web, rendición de cuentas como son las memorias institucionales.

Principio 29 – Utilización abusiva de servicios financieros	Se cumple completamente, existen los mecanismos para controlar la información en base a listas nacionales e internacionales, además de sistemas de monitoreo transaccional

De acuerdo al análisis todos los principios se cumplen, y al momento se han sustentado estos en el nuevo Código Orgánico Monetario y Financiero.

CONLUSIONES

Al finalizar el presente trabajo se tiene las siguientes conclusiones:

- Las instituciones financieras en un nuestro país tiene un alto grado de control a nivel de los organismos como son el Banco Central del Ecuador, la Superintendencia de Bancos y la Junta Política y Regulación Monetaria y Financiera, producto de este control se han emitido varias regulaciones que intentan asegurar los procesos de la Banca.

- La resolución JB-2012-2148 exige la implementación de esquemas de seguridad en los canales electrónicos los cuales son aplicables únicamente a las entidades controladas por la Superintendencia de Bancos.

- Los organismos de control están más enfocados en la Banca y existe menos control en las cooperativas generando grandes brechas en el sistema financiero.

- Los mecanismos de seguridad aplicados de acuerdo a la resolución JB-2012-2148, incrementaran la seguridad de los canales electrónicos, sin embargo en temas de seguridad lo que se hace es mitigar el riesgo mas no existen canales 100% seguros.

- La aplicación de mecanismos de seguridad en Banco Pichincha han permitido disminuir un 48% del valor pagado por fraudes según la memoria institucional de este Banco.

- Las personas o grupos que se dedican a realizar fraudes en canales normalmente lo hacen sobre las instituciones financieras más grandes dado que el impacto del fraude va a ser mayor y probablemente con el mismo esfuerzo de hacerlo en un banco pequeño

RECOMENDACIONES

- Se recomienda que las seguridades en los canales electrónicos se apliquen de tal forma que esto no afecte a la usabilidad de los clientes dado que al afectarla se dejara de usar los mismos y la tendencia actual es la de trabajar en canales electrónicos, evitando las colas de atención.

- Las instituciones del sistema financiero deben emprender en campañas que permitan educar a los clientes en buenas prácticas de seguridad financiera para disminuir los fraudes en sus canales.

- Se recomienda que las instituciones financieras ejecuten sus proyectos para cumplimento de la norma y que lo vean como un valor para el cliente por lo cual deben cuidar que su aplicación este correctamente socializada para evitar la disminución del uso de los canales.

BIBLIOGRAFÍA

Aguirre, Jorge. *Libro Electrónico de Seguridad Informática y Critografía*. UPM, 2006.

Astudillo, Karina. «slideshare.» 12 de 11 de 2013. <http://es.slideshare.net/kastudi/prevencin-de-fraudes-electrnicos>.

Banamex, Portal. «Fraudes electrónicos - como protegerte.» *GestioPolis* (2005): http://www.gestiopolis.com/canales5/comerciohispano/59.htm.

Basilea, Comité de Supervisión Bancaria de. *Principios Básicos para una supervisión bancaria eficaz*. 2011.

Cáceres, Diego. «Seguridad en sistema bancario.» *EL TIEMPO* 18 de 03 de 2013: http://www.eltiempo.com.ec/noticias-cuenca/117924-seguridad-en-sistema-bancario/. <http://www.monografias.com/trabajos14/banca-electronica/banca-electronica.shtml>.

Chavéz J, Jorge. *Estudios Generales-Infomática Básica*. Senati, 2012.

Cuellar, María Mercedez. «Mitigar el riesgo de fraude es un desafío para las autoridades, la banca y los usuarios.» *Semana Económica* (2012): 10.

Diario, El. «La Fiscalía ha recibido 1.360 denuncias por fraude informático este año.» *El Diario* 03 de 05 de 2011: http://www.eldiario.ec/noticias-manabi-ecuador/200348-la-fiscalia-ha-recibido-1-360-denuncias-por-fraude-informatico-este-ano/.

Ecuador, Asociación de Bancos Privados del. *Asociación de Bancos Privados del Ecuador*. 03 de 2012. 07 de 2014. <http://www.asobancos.org.ec/seguridad.htm>.

Ecuador, Derecho. *Derecho Ecuador*. s.f. 22 de 07 de 2014. <http://www.derechoecuador.com/servicio-al-usuario/diccionario-juridico/diccionario-juridico--de-?l=F>.

Memoria, Banco de Loja. «http://www.bancodeloja.fin.ec:8080/Portals/0/memoria2013-High-small.pdf.» 2013. *http://www.bancodeloja.fin.ec:8080/Portals/0/memoria2013-High-small.pdf.*

Memoria, Banco Pichincha. «https://www.pichincha.com/portal/Portals/0/2013%20Informe%20Anual%20y%20Memoria%20de%20Sostenibilidad.pdf.» 2013.

O'Higgins, Jorge. «Gestión de seguridad en canales electrónicos .» (2009): http://www.fiuba6662.com.ar/6648/extras/2009_Charlas/Charla_Johiggins_fiuba.pdf.

Produbanco. «http://200.24.195.133/GFPNet/descargas/memoria_anual2013.pdf.» 2013.

Salazar, Andrea. «http://canal-tecnologico.com.» 28 de 01 de 2011. <http://canal-tecnologico.com/index.php?option=com_content&view=article&id=622:robar-lo-que-sea-y-a-quien-sea-delitos-informaticos-en-el-ecuador&catid=25:soft&Itemid=54>.

SIB. *Superintendencia de Bancos y Seguros del Ecuador*. s.f. 21 de 12 de 2014.

Slayer, Hoax. *Hoax Slayer*. s.f. 15 de 07 de 2014. <http://www.hoax-slayer.com/atm-skimming.html>.

Slideshare. *Slideshare*. 23 de 07 de 2009. <http://es.slideshare.net/martinn2/que-es-seguridad-electrnica>.

Superintendencia de Bancos y Seguros del Ecuador. «Normas Generales para las instituciones del sistemas financiero.» (s.f.).

Universo, El. «Bancos pagaron a clientes en 2 mil casos de fraude virtual.» *El Universo* 26 de 11 de 2013: http://www.eluniverso.com/noticias/2013/11/26/nota/1821096/bancos-pagaron-clientes-2-mil-casos-fraude-virtual.

Wikipedia. *Wikipedia*. s.f. <http://es.wikipedia.org/wiki/Banca_electr%C3%B3nica>.

Zweicon. *Zweicon*. 23 de 07 de 2014. <http://www.zweicom.com/index.php?page=gateway-ussd>.

ANEXOS

ENCUESTA DE CANALES ELECTRÓNICOS

1. ¿Indique de que institución financiera es cliente?

☐ Banco de Loja

☐ Banco de Pichincha

☐ Produbanco

☐ Otra

2. ¿Utiliza usted los canales electrónicos de su banco?

☐ Si

☐ No

3. ¿Cuál de los siguientes canales electrónicos utiliza?

☐ Cajero Automático

☐ Telemático

☐ Banca Electrónica

☐ Banca Móvil

4. ¿Considera usted que los canales electrónicos son seguros?

☐ Si

☐ No

5. ¿Los canales electrónicos de su Banco son fáciles de utilizar?

☐ Si

☐ No

6. ¿Ha sido víctima de un fraude en canal electrónico?

☐ Si

☐ No

7. ¿Cuál es el mecanismo para acceder en el canal electrónico de su Banco?

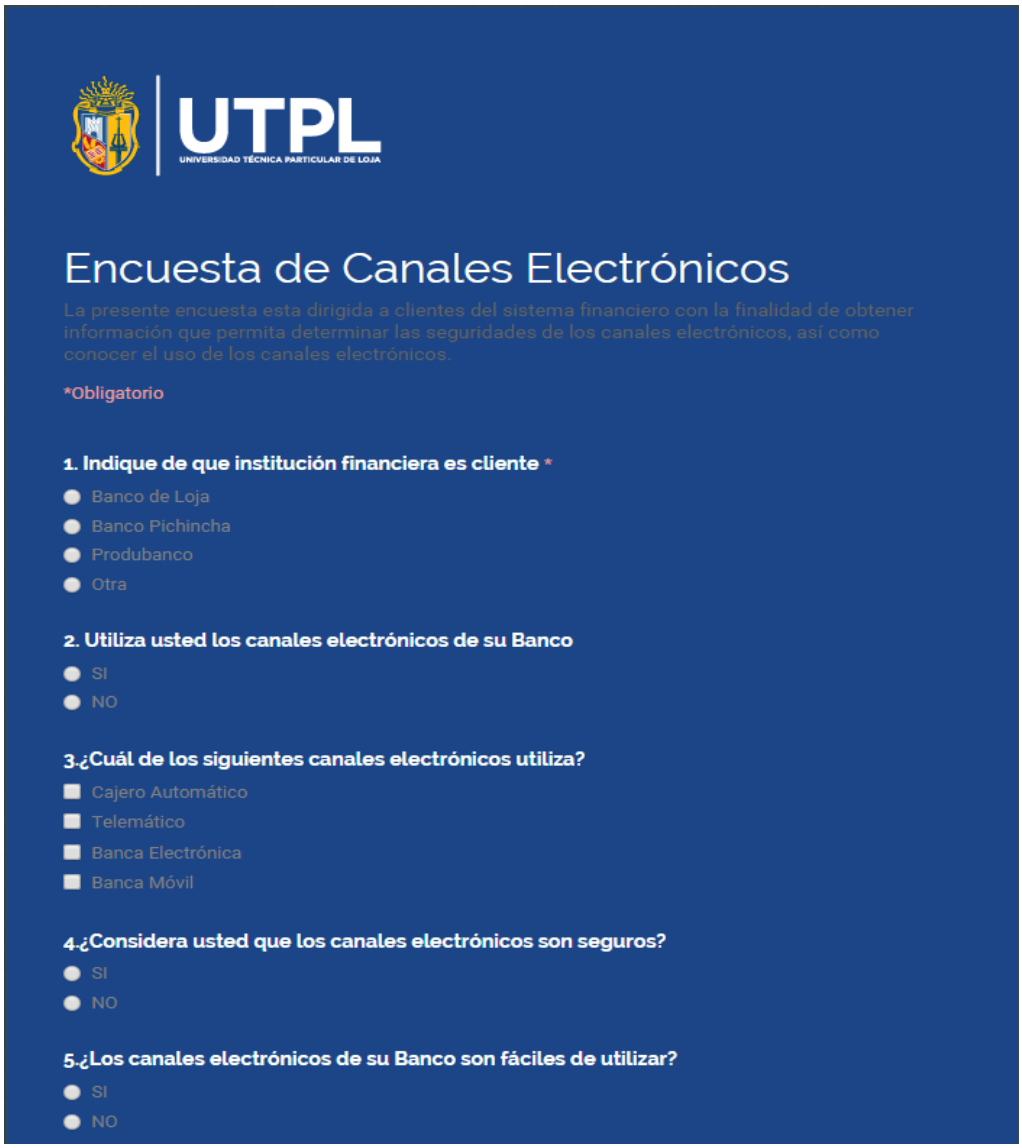
	Clave	**Imagen y Pregunta**	**Código de verificación SMS (OTP)**	**Tarjeta de coordenadas**	**Ninguno**

Cajero Automático	☐	☐	☐	☐	☐
Banca Electrónica	☐	☐	☐	☐	☐
Banca Móvil	☐	☐	☐	☐	☐
Telemático	☐	☐	☐	☐	☐

8. ¿Cuál es el mecanismo para realizar transacciones en el canal electrónico de su Banco?

	Clave	**Imagen y Pregunta**	**Código de verificación SMS (OTP)**	**Tarjeta de coordenadas**	**Ninguno**
Cajero Automático	☐	☐	☐	☐	☐
Banca Electrónica	☐	☐	☐	☐	☐
Banca Móvil	☐	☐	☐	☐	☐
Telemático	☐	☐	☐	☐	☐

Formulario de Encuesta Publicado



UTPL
UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta de Canales Electrónicos

La presente encuesta esta dirigida a clientes del sistema financiero con la finalidad de obtener información que permita determinar las seguridades de los canales electrónicos, así como conocer el uso de los canales electrónicos.

*Obligatorio

1. Indique de que institución financiera es cliente *

- Banco de Loja
- Banco Pichincha
- Produbanco
- Otra

2. Utiliza usted los canales electrónicos de su Banco

- SI
- NO

3.¿Cuál de los siguientes canales electrónicos utiliza?

- Cajero Automático
- Telemático
- Banca Electrónica
- Banca Móvil

4.¿Considera usted que los canales electrónicos son seguros?

- SI
- NO

5.¿Los canales electrónicos de su Banco son fáciles de utilizar?

- SI
- NO