República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Trabajo de Titulación

Para la Obtención del Título de:

Ingeniera en Telecomunicaciones

Tema:

Análisis del desempeño de los mecanismos de seguridad en los canales electrónicos de la banca virtual de un banco en la ciudad de Guayaquil.

Autora:

Andrea Katherine Logroño Carrión

Director del Trabajo de Titulación:

Ing. Diego Aguirre González, Met.

2022

Guayaquil - Ecuador

AGRADECIMIENTO

A mi Dios, a mi familia y a mis amigos que estuvieron de manera directa en el apoyo a la resolución de este estudio.

DEDICATORIA

Va dedicado a mis padres, y mis hermanos que de una u otra manera estuvieron en apoyo constante para poder salir adelante.

La responsabilidad de este trabajo de investigación, con sus resultados y conclusiones pertenece exclusivamente al autor.

Andrea Katherine Logroño Carrión

ANÁLISIS DEL DESEMPEÑO DE LOS MECANISMOS DE SEGURIDAD EN LOS CANALES ELECTRÓNICOS DE LA BANCA VIRTUAL DE UN BANCO EN LA CIUDAD DE GUAYAQUIL.

Andrea Katherine Logroño Carrión
andrealogrono7@gmail.com

RESUMEN

El siguiente trabajo comprende un análisis estructural de un banco de la ciudad de Guayaquilsobre el cual se hace un estudio a profundidad en cuanto a la organización interna de seguridad que se encuentra implementada dentro de la banca, con el fin de obtener información que permita hacer sugerencias y observaciones de los mecanismos empleados para asegurar al cliente la confidencialidad y buen manejo de sus datos.

Para tener un buen análisis se detallaron cada uno de los involucrados de manera descriptiva que junto con la encuesta permite entender la situación actual de la banca y su relación de confianza con el cliente. Cada una de las recomendaciones de seguridad que se anotaron han sido pensadas con el fin de mejorar las vulnerabilidades que fueron encontradas. Se sugiere implementación de procesos y protocolosde seguridad en cuanto a la parte de redes; implementación de firewall, nueva reestructuración de red en las oficinas que manejan los datos vulnerables.

Palabras clave: Banca Virtual, Seguridad, Vulnerabilidad.

INTRODUCCIÓN

La seguridad bancaria en los últimos tiempos ha tenido que mejorar sus parámetros con el fin de brindar completa confidencialidad a los clientes afiliados. Debido a que nos encontramos en un mundo tan cambiante con avances tecnológicos que crecen de manera agigantada, han obligado a la banca en mejorar la experiencia del cliente en cuanto a los servicios que ofrecen.

Sin embargo, así como avanza la tecnología en pro de mejorar servicios y hacerlos más accesibles a la comunidad cibernética afiliada a la banca, se desarrollan potenciales enemigos virtuales que se encuentran en constante búsqueda de perpetrar e incluso vulnerar los mecanismos de seguridad que se encuentran implementados por la banca.

El análisis realizado a la banca acerca de los mecanismos de seguridad sobre los cuales se encuentra trabajando y brindando seguridad a sus clientes, nos permitió conocer desde el nivel físico hasta nivel de red la estructura y el alcance que tiene cada uno de sus parámetros. Los que nos dejaron conocer que pueden darse mejoras a ciertos procesos, eliminar ciertos permisos que pueden poner en riesgo la información, entre otras que se detallaran en lo que se desarrolla el artículo.

Después del análisis se procedieron a realizar las recomendaciones que se espera en análisis lleguen a ser implementadas estructuralmente y así permitan mantener un buen nivel de seguridad para los clientes afiliados, con el fin de conservar los estándares de calidad ofrecidos por la banca sin ser blancos posibles a vulnerabilidades.

Durante los últimos años la banca ha jugado un papel importante para la economía del Ecuador. Según la corporación nacional de finanzas populares y solidarias en su boletín de sistema financiero, en diciembre 2020 informaba que a la fecha la banca llegó a generar 48 millones de dólares, los cuales representaban un crecimiento de más del 8% con relación al 2019 donde apenas se alcanzó los 3 millones de dólares, simbolizando así, un ente favorabledebido a su alta liquidez en comparación al 2019.

La banca al ser un intermediario financiero para los clientes y manejar fondos monetarios dedistintas maneras; se ha vuelto influenciado por el ambiente tecnológico que lo obliga a involucrarse de manera directa con el fin de brindar un servicio ágil y amigable al cliente en cuanto al uso de las tarjetas de débito y crédito. Sin embargo, ante las mejoras tecnológicas estas van de la mano con personas que buscan sacar provecho de esto, lo cual ha generado lanecesidad de crear recursos de seguridad para garantizar un

buen manejo entre los involucrados; cliente banca y transacción virtual.

Cada uno de los recursos que se aseguran por parte de la banca virtual son regulados por la superintendencia de bancos, la misma que tiene como misión velar por cada uno de los derechos que tienen los usuarios en los servicios que son ofrecidos por las entidades bancarias.

El actual crecimiento tecnológico mundial y la demanda de canales electrónicos, ha puesto ala banca virtual a buscar la manera de brindar servicios que generen confianza al usuario. Así como avanzan los requerimientos tecnológicos, aparecen nuevos obstáculos, como son los denominados ciberataques que ponen en riesgo los datos que se manejan de manera virtual con el fin de hacer uso indebido de los mismos.

Para la banca, esto genera una obligación con el cliente en proveer mecanismos de autenticación en estos canales, y tener un buen manejo de la información recopilada con el fin de garantizar que todo lo recopilado se mantiene y mantendrá en un estado de confidencialidad y sin distribución a terceros por ningún medio.

Los canales electrónicos que comprenden de la banca virtual se pueden deslingar las transacciones, pagos de tarjetas, compras en línea entre otras que se integran por parte de la banca virtual. Cada uno de los mencionados al manejar información confidencial de cada usuario, requieren una protección que el banco deberá implementar y asegurarse del buen desempeño de estos.

¿Los mecanismos existentes de seguridad manejados por la banca virtual, son suficientes paragarantizar al usuario la confidencialidad de su información?

OBJETIVOS

2.1. Objetivo general

Analizar los mecanismos de autenticación-seguridad provistos por la banca virtual en los canales electrónicos que se proveen.

2.2. Objetivos específicos

- Detallar los mecanismos de seguridad que se encuentran implementados por la banca para su eficiencia en su banca virtual.
- Describir los posibles ataques cibernéticos que la banca virtual como sus mecanismos están expuestos.
- Establecer mejoras de seguridad para el buen desarrollo y manejo de datos de la

banca virtualpara con sus clientes.

MARCO TEÓRICO

En un mundo globalizado los países del primer mundo, la banca virtual fue una de las practicas más comunes en ser puestas en marcha, donde el acceso a la información bancaria era por medio de smartphones, computadoras y de esta manera poder realizar cualquier tipo de transacción para algún pago o tener acceso a algún servicio bancario que el banco provea.Los registros de clientes asociados a un software de una banca datan del año 1995 en Wells Fargo (banca perteneciente a Estados Unidos) donde se podían ya realizar transacciones bancarias explica. (Seybold & Marshak, 1997).

Sin embargo, para los países latinoamericanos según un estudio realizado por la OEA (organización de estados americanos) en el 2017, el comportamiento de los clientes y la infraestructura en seguridad cibernética difieren. Por lo cual para el 2017 solo apenas un 24%había hecho transferencias entre cuentas de manera virtual. Una de las razones por las cualesse evidencia un porcentaje bajo a inicios del 2017 fue los ataques de seguridad cibernética que se daban a las distintas entidades bancarias por varios métodos.

En el Ecuador, las instituciones bancarias han sido puesta en evidencia que las largas filas y clientes esperando son característica que sigue persistiendo hasta la actualidad; a pesar de que el país ya está disponible la banca virtual por parte de varios bancos reconocidos a nivel nacional. El temor por la vulnerabilidad a la información sigue persistiendo por lo que los canales comunes de presencia física donde interactúa el cliente y el sujeto bancario con documentación requerida para validar que las transacciones sean seguras sigue siendo la másrecurrente por personas cuyo acceso a la tecnología es limitado.

La super intendencia de bancos en el 2016 aclaraba que 23 bancos existentes han sido calificados de acuerdo con el riesgo controlado, destacándose Banco de Guayaquil, Banco Pichincha, los cuales tienen un sistema asegurado de banca electrónica proveyendo a los clientes y asegurando la confidencialidad de su información en los servicios provistos por la banca, cumpliendo con los requerimientos mínimos para poder impulsar su banca de maneravirtual. (Carolina, 2017).

A pesar de contar con varios parámetros a ser cumplidos por la entidad bancaria, la malversación de información, vulnerabilidad, e incluso rompimiento de

confidencialidad de la data manejada por la mencionada ha sido de cierta manera atacada por ciberataques. Para mayo del 2021 se enunciaban que se habían cometido para ese año, cerca de 600 delitos cibernéticos, donde para el mes de octubre uno de los casos más relevantes se desencadenaría(el ataque cibernético al Banco Pichincha el 9 de octubre).

En los reportes de seguridad de ESET del 2021 se han realizado casi más de 140 mil detecciones de vulnerabilidad en software de los bancos. Siendo de gran preocupación para las entidades que urgen en la necesidad de mejorar los sistemas seguridad.

3.1. Agente regulatorio del sistema financiero

En el Ecuador quienes estipulan normas a ser aplicadas por parte de los sectores financieros sean públicos o privados es la Super Intendencia de Bancos, la cual vela por una buena administración. Siendo así, en la sección 8 de la Norma de Control Para las Entidades De Los Sectores Financieros Público y Privado, en el artículo 17 literal n, se invita a la banca privadaa que se implementen controles y mecanismos que garanticen la seguridad de cada uno de susclientes.

Determinar el riesgo que puede darse en las transacciones de los clientes que incluyanel movimiento del dinero en canales electrónicos, con el fin de evitar algún acto fraudulento que ponga en riesgo la información o bienes del cliente. A esta norma se suman los dos literales siguientes o y p que deben ser bloqueados los canales electrónicos en cualquier momento en que se registre algún intento fallido o situación inusual que, de manera inmediata,deberá ser notificada al cliente por cualquier medio de contacto que este encuentre anexado; todo esto bajo la "Codificación de las Normas de la Superintendencia de Bancos" estipulado.

3.2.Revisión bibliográfica

3.2.1. Banca Virtual

Es un servicio que las entidades bancarias ofrecen a sus clientes, con el fin de poder facilitar las transacciones operacionales bancarias. Desde la verificación de la cantidad de dinero que posee el cliente, hasta realizar pagos y transferencias; sean estas en un comercio en línea o hacia otra persona. (Antonio, 2016)

3.2.2. Comunicación segura entre cliente y banca virtual

Se define como una buena comunicación o intercambio de información, cuando existe una comunicación segura que ha cumplido con los requerimientos de seguridad básicos. El bancoinicia por recopilar información compartida por el usuario de manera

encriptada, el cliente de proveer cada uno de los campos obligatorios y que estos sean emitidos solo por él y no por cualquier persona. Una vez intercambiada la información el acceso deberá ser aprobado y no negado. (Rosse, 2015)

3.2.3. Delitos informáticos

Es aquella información que ha sido afectada, así como el dato jurídicamente protegido, en otras palabras, la información que una persona tiene dentro de su cuenta de correo y el dato de la cuenta bancaria protegido, entre otros que están protegidas por la ley.

3.2.4. Phishing

El phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder defuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad manipulan el receptor para robar información confidencial.

3.2.5. Ataque cibernético

Conocida como una acción malintencionada que tiene como fin apropiarse de información única y privada para hacer un mal uso de esta o pedir dinero a cambio por recuperarla.

MARCO METODOLÓGICO

4.1. Nivel y alcance de la investigación

El presente trabajo estará suscrito bajo un nivel perceptual donde la investigación tiene comofinalidad describir los mecanismos de autenticación que la banca virtual en sus generalidades emplea para el cliente y cuan seguros son los mismos, cuyo tipo de investigación será descriptivo totalmente.

La investigación tiene como alcance lograr analizar los mecanismos de autenticación de tal manera que se puede entender la eficiencia de cada uno de estos, ejecutados por la banca virtual en función de satisfacer las necesidades del cliente y asegurar la confidencialidad de sus transacciones, sumado a esto la forma en cómo se almacena toda la información recopilada.

4.2. Diseño de la investigación

La investigación estará formulada bajo un concepto descriptivo que permita conocer los mecanismos de seguridad empleados por el banco de estudio.

4.3. Población muestra y unidades de estudio

En base al Banco en análisis se estimará una población que resida en la ciudad de

guayaquil y sea cliente de este. Con el fin de estudiar a un grupo en concreto, se buscará definir la cantidad de usuarios que hagan uso de la banca virtual con la finalidad de conocer si estas hanpasado por algún problema en cuanto a la seguridad y confidencialidad de sus credenciales alhaber ejecutado alguna transacción en la banca virtual.

Para este análisis se identificó a la población perteneciente al banco en estudio que se encuentra afiliada a la banca virtual residiendo en la ciudad de guayaquil. Se cuenta con una población de 601 personas adheridas a la banca virtual del banco en estudio.

4.4. Técnicas e instrumentos de recolección de datos

Al ser una investigación descriptiva con base fundamentada en un análisis de los clientes asociados a la banca virtual. Se busca que por medio de la encuesta con un cuestionario de preguntas se logre recolectar información necesaria que evidencié la necesidad de estar constantemente modernizando los mecanismos de autenticación de los canales electrónicos de la banca virtual.

Así mismo por medio de la entrevista con profesionales del área de supervisión de los controles de seguridad implementados, bajo un cuestionario guiado se buscará entender un poco más lo fundamental que es un buen manejo de los servicios de autenticación y de ser elcaso anotar ciertas recomendaciones que aporten a este trabajo investigativo.

4.5. Infraestructura general del Banco

Sus conexiones son de manera directa, hacia las distintas sucursales que se manejan y con Banred el cual es quien procesa las transacciones con las tarjetas. A nivel de banco, se realizó un estudio en el segmento de red en cuanto a una de las principales VLAN´s sobre la que se encuentran equipos de la red corporativa conectados; es decir de unade las estaciones de trabajo.

Dentro de una de las VLAN´s se encuentran los ATM´s y al no haber restricciones de tráfico de ninguna índole hace que la red corporativa este en el alcancede la red de los servidores donde están los equipos que reciben los datos de los ATM´s encargados de recibir los datos para las autorizaciones.

Para mantener conexión con las otras sucursales, la conexión se realiza mediante canales dedicados de MPLS con un segmento aparte para la conexión hacia Banred.

4.6. Detalles de almacenamiento de red

Con el objetivo de que esto se cumpla, se espera y recomienda que cada uno de los servidoresestén cifrados y así minimizar el riesgo de que al momento de traspasar la información por lared vaya sin cifrar.

Proveedores con los cuales la compañía comparte datos de tarjeta. El banco trabaja en conjunto con los siguientes proveedores de servicio y soporte que manejanlos datos de la tarjeta y el vínculo asociado con la banca virtual para transacciones virtuales.

Tabla 1. Proveedores de soporte al banco

Banred	Procesador
G4s	Almacenamiento y transporte de cintas
CNT	Proveedor de servicios de comunicaciones
Multiservice	Desarrollo de software y soporte a la aplicación Switch de transacciones.

Elaborado por: Autora

4.7. Protección perimetral

La infraestructura actual del banco a nivel de protección perimetral es basada en un firewall que controla el tráfico tanto entrante como saliente de internet. En nivel de red interna se cuenta con segmento donde están los servidores protegidos por un firewall interno y otro donde están las estaciones de trabajo existentes. En este mismo segmento mencionado están los ATM´s de la sede principal, en las sucursales no existe segmentación y sus estaciones detrabajo como los ATM´s se encuentran mezclados.

4.8. Elementos para considerar

Debido a que no se cuenta con redes inalámbricas aun implementadas, lo ideal es que desde allí se restringa el acceso a los sistemas que manejan la información de tarjetas o equipos en el alcance y estas se puedan segmentar de las demás redes por medio de un firewall o un equipo que cumpla con las características esenciales de firewall y así prohibir desde esas redesel tráfico hacia la red PCI. Por lo que el router de la izquierda será el encargado de limitar estetráfico a través de las listas de acceso, negando todo el tráfico con destino a la red PCI. De esta manera es importante recordar que PCI considera las redes inalámbricas totalmente inseguras. (como si fueran internet) y debido a esto, no pueden estar de manera directa, sino que debe ser realizado intermediadas por un firewall.

Tener equipos como servidores y estaciones de trabajo sin una buena

segmentación implica un alcance mayor y la implementación de al menos los siguientes controles sobre todo esos equipos generando costos adicionales y tiempos altos de instalación, así como su configuración.

Configuración segura" hardening" del equipo para así garantizar que no son del todovulnerable desde el cual se pueden generar ataques hacia los servidores principales donde estén los datos de tarjeta o a la red en donde se encuentra.

- Configuración adecuada de logs, junto a su custodia centralización y análisis de los eventos diarios.
- Realizar un buen escaneado de las vulnerabilidades y pruebas de penetración.
- Sistema de monitoreo integral de archivos FIM (File integrity monitor) o control decambios.
- Implementación de parches en un tiempo corto.
- Manejo de roles autenticación y perfiles siguiendo los requisitos de PSI.

La revisión que se realizó es basada en un esquema de defensa en profundidad para así poderfacilitar el entendimiento y la definición e implementación de un plan de trabajo que permita un mejor nivel de seguridad dentro de la compañía en este caso se analizaron los siguientes aspectos.

- Procesos
- Nivel físico
- Nivel de red
- Configuración de equipos
- Configuración de aplicaciones y desarrollo
- Personal y terceros
- Políticas y procedimientos

ANÁLISIS Y RESULTADOS

5.1 A nivel de procesos.

Es de alta importancia identificar los procesos que se manejan en cuanto a la información detarjetas y los sitios donde se almacenan o se transmiten de forma lógica o física. A raíz de estos procesos se identifican los servidores, estaciones de trabajo, equipos de red (enrutadores,switches, firewalls).

5.2. Oportunidades de mejora recomendadas

Es recomendable generar un diagrama de red general donde se logre entender de manera rápida los segmentos de red en donde existen los sistemas en el alcance, la DMZ, las conexiones dedicadas con otras entidades, las redes inalámbricas y los firewall o equipos de red que manejan la segmentación.

Hay que evaluar qué método de seguridad se va a usar en cuanto a las tarjetas si se desea truncar que es almacenar máximos 26 primeros y los cuatro últimos dígitos O si se desea enmascarar lo que es que es almacena de manera completa del dato y solo se muestra en la pantalla una porción. Cabe mencionar las diferencias entre truncar y enmascarar cuando se enmascara es decir que el dato está almacenado de manera completa y solamente se mostrará una porción mientras que si se trunca quiere decir que está almacenado sin el número completo sean los 6 primeros y los cuatro últimos como se mencionaba anteriormente con locual no sería necesario cifrar el archivo.

Es importante recordar que los datos deben ser cifrados de la tarjeta en cualquier sitio dondese mantengan así sea de manera temporal en el caso de que no se pueda cifrar el archivo se debería hacer un cifrado del disco.

Debe ser eliminado de forma segura con aplicaciones que cumplan con los estándares de eliminación de archivos todos los datos de las tarjetas que se tengan actualmente en los diferentes servidores o estaciones de trabajo es recomendable realizar una búsqueda de datosde tarjeta por De software para poder identificar posibles sitios con datos de tarjeta no controlados.

Así mismo, evaluar la posibilidad de automatizar los procesos para que no requiera Intervención humana de esta manera disminuir los puntos en los cuales está manejando datosde la tarjeta por terceros.

5.3. A nivel de seguridad Física

Se tiene controles de acceso físico a las instalaciones en especial al centro de datos. Se tiene implementado un esquema de defensa a través de los controles de acceso que han sido establecidos propiamente por el banco, siendo los siguientes.

- Control de visitantes, toma a qué persona se visita, la fecha y su identificación.
- Cámaras que controlan el centro de datos
- Acceso biométrico para el acceso al centro de datos.
- Protección a los sitios donde están los equipos de comunicaciones siendo los

puntosde acceso inalámbricos, switch, etc.).

- Existe un almacenamiento en cintas en un lugar remoto de forma segura.
- Para el control de las cintas, se realiza un inventario

5.4. Oportunidades de mejoras identificadas.

- Mantener la idea de aumento de la capacidad de grabación del sistema de cámaraspara almacenar la información, por un periodo que exceda los 90 días
- Mejorar las políticas de acceso para visitantes y empleados.
- Los accesos deben ser distintos en cuanto a los visitantes y los empleados.
- Que la bitácora que es utilizada para llevar el registro de visitantes sea llenada demanera frecuente.
- Políticas de ingreso y egreso de equipos electrónicos, debe ser bajo control estricto.
- Los medios seguros para la destrucción de los medios físicos deben ser especificado,puesto que se manejan.
- Las cintas de respaldo que contengan los datos de las tarjetas se deben cifrar, o en cierto caso de no ser requeridos deben ser eliminados de forma segura. Si no se pueden cifrar, y estos datos son requeridos; se debe establecer unos controles adicionales parael acceso a las cintas y su información almacenada. Esta debe de venir de una autorización previa de la empresa que deje en constancia cuando se hayan dado las autorizaciones.
- En la sala de reunión se encontraron puntos de red que han sido habilitados, dando libertad a los visitantes para conectarse a la red interna sin previa autorización. Para esto se recomienda que se implementen controles adicionales. Como la implementación de un sistema de control de acceso de red (NAC) o una solicitud de autenticación antes de la asignación de una IP.

5.5. A nivel de red

Todos los equipos que se encuentran en el alcance deberán de cumplir con los siguientes requerimientos de manera global.

El primer requisito es orientado a definir una arquitectura de seguridad y establecer restricciones a lo mínimo social como según los requisitos está definir e implementar equiposde red basados en cierto estándar de configuración seguro como los definidos por los sitios de seguridad o NIST. Realizar una transmisión de información de

forma cifrada en redes inalámbricas, hacer una actualización del sistema periódico, así como definir roles y perfiles para el manejode usuarios y contraseña.

Realizar un registro de auditoría y sincronización de la hora NTP, realizar un escaneo de las redes inalámbricas no autorizadas, así como de las vulnerabilidadescon pruebas de penetración IDS/IPS.

5.6. Observaciones encontradas.

Se tiene implementado un esquema de defensa perimetral que permite controlar el tráfico que sea saliente es decir que cuenta con un Firewall externo.

No se tiene en redes inalámbricas y los roles y perfiles de los usuarios de los equipos de red están documentados.

Para cada segmento de red con los que se cuentan se tiene las ips monitoreando, este monitoreo se debe mantener de los segmentos en el alcance y el internet una vez que se implemente la disminución de este. Se tiene implementado acceso remoto con doble factor de autentificación por medio del certificado y contraseña.

5.7. Oportunidades de mejor identificadas

Se debe depurar y dejar documentar la justificación de las reglas actuales para permitir únicamente el tráfico requerido para la operación ya que se tienen los muy abiertos o con máspermisos de los que se requiere.

Se debe realizar una revisión semestral de las reglas del firewall y configura para evitar ataques especializados

Las contraseñas están compartidas por varios administradores y se tiene escrita y protegida en el sobre por el área de seguridad se recomienda usar cuentas propias y no compartidas y así poder identificar en cada momento quien fue responsable de las acciones ejecutadas en losequipos el área de seguridad también puede tener un usuario diferente con la contraseña protegida sobre que permite identificar cuando ha sido abierto.

Se deben implementar controles para minimizar la posibilidad de conexión de equipos noautorizados en la red.

5.8. A nivel de servidores y estaciones de trabajo.

Todos los servidores y las estaciones de trabajo que están involucradas en al alcance deben con los requisitos que de manera global se detallan a continuación:

- Realizar de manera periódica actualizaciones del sistema y controles de cambios

de perfiles y roles. Tener un buen manejo del usuario y sus contraseñas respectivas.

- Realizar un escaneo de vulnerabilidad mediante pruebas de penetración.

5.9. Oportunidades de mejoras identificadas.

Configurar todos los equipos en el alcance de forma segura basándose en los estándares de configuración hardening. Se debe implementar conexiones seguras (cifradas) cuando se usa terminal Services. Implementar antivirus sobre los sistemas NUX en el alcance o implementar controles adicionales que minimicen los vectores de ataque que son protegidos por el AV.

Implementar procesos de actualización de parches en base a los requeridos en PCI sobre todolos sistemas en el alcance incluyendo a los servidores y las estaciones de trabajo.

De manera anual se deberán hacer pruebas de penetración internas y externas incluyendo la parte de las aplicaciones. Implementar un sistema de file integrity monitor sobre los servidores y sus estaciones de trabajo en el alcance para así poder identificar cambios no autorizados sobre los archivos delsistema y otros importantes como en el que se maneja las configuraciones y aplicaciones.

5.10. A nivel de personal, terceros y políticas.

Se considera a las personas empleados del banco como parte fundamental en cuanto a mantener la seguridad de los sistemas, las aplicaciones y en el manejo de la información en cuestión. Se puede lograr minimizar los riesgos de perdida de información, pero si las personas no estánconcientizadas en cuanto a la importancia de la seguridad en los diferentes niveles, se puedendar perdidas de información.

5.11. Oportunidades de mejoras identificadas:

Los administradores encargados no cuentan con conocimiento en seguridad y las configuraciones seguras sobre los equipos a cargo. Los administrados deben contar con los conocimientos de seguridad que aseguren un buen manejo tanto a nivel de configuración del sistema y de sus aplicaciones que sobre el equipo que se tiene a correspondencia.

Para los terceros no se han definidos los roles y sus obligaciones en cuanto a la protección dela información. Por lo que se espera que se los integre a la auditoria del banco

y que quede enevidencia el cumplimiento anual. Validar cada uno de los procesos y servicios contratados sobre los que se manejan los datos del cliente.

5.12. Compensaciones de seguridad

Definir de manera correcta la ubicación de los sitios donde se manejará la información de tarjeta, sus datos y de qué manera se busca protegerlos. Determinar de cierta manera cuales son las mejores opciones en cuanto al manejo de la información (cifrarla, eliminarla conformepasa el tiempo o un Hash) para esto la información que se desee eliminar deberá ser de formasegura, usando herramientas como PGP SHRED, ERASER, etc).

Se realizo una encuesta a una muestra de 341 clientes que se encontraban afiliados al banco de la ciudad de guayaquil; proviniendo de una población de 601 clientes.

En cuanto a la ***pregunta 1*** donde se interroga si el cliente hace uso de la banca virtual, los resultados arrojaron que una gran parte de los asociados al banco utilizan banca virtual, siendoun 92%.

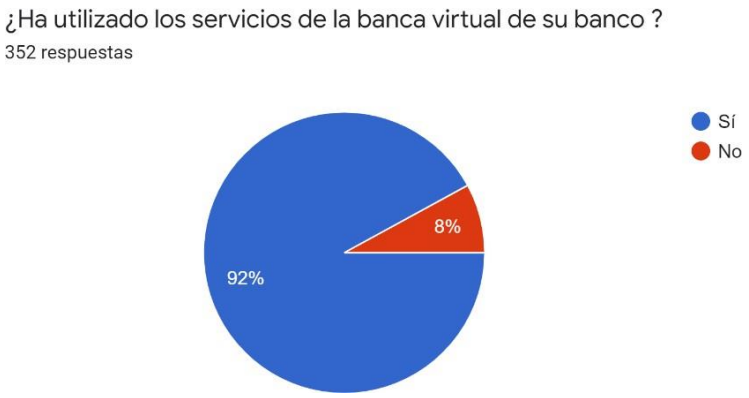

Ilustración 1
Autora: Andrea Logroño

Siguiendo a esta encuesta, en la ***pregunta 2*** se determinó, que de los métodos de seguridad empleados de los más destacados está el código de seguridad con límite de tiempo con la representaciónde un 33%, mientras que los menos seguros para los clientes termina siendo la huella dactilar.

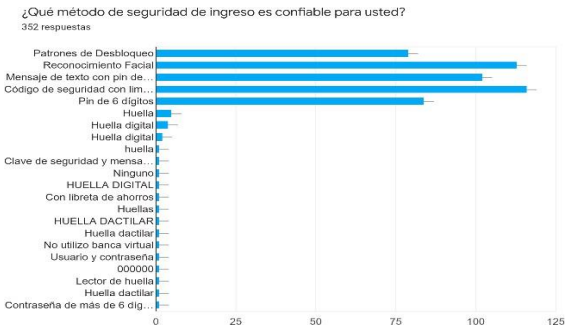

Ilustración 2

Autora: Andrea Logroño

Para la ***pregunta 3*** los clientes aseguran que el método de ingreso que ha sido determinadopor cada uno es seguro para su banca. Sin embargo, casi un 12% no lo considera seguro.

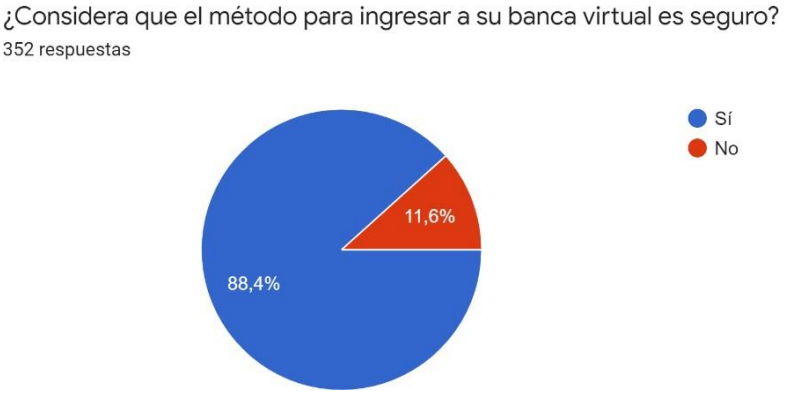

Ilustración 3

Autora: Andrea Logroño

En la ***pregunta 4*** así mismo casi un 45% no considera confiable a la seguridad empleada por parte de la banca virtual.

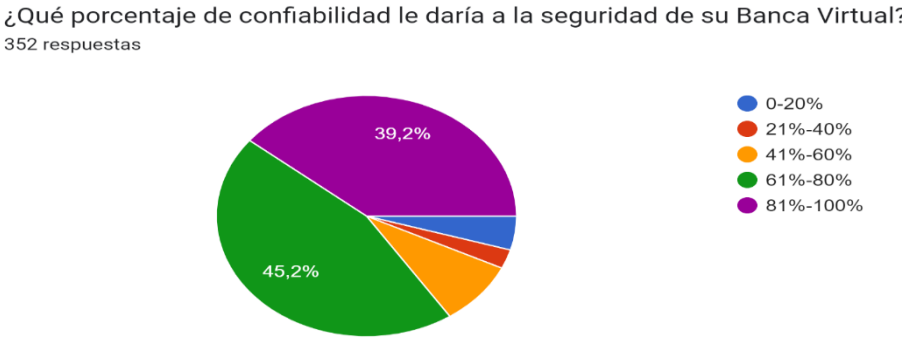

Ilustración 4

Autora: Andrea Logroño

CONCLUSIONES

La banca virtual puesta en análisis siempre ha buscado estar en constante innovación y crecimiento tecnológico para brindar facilidades a sus clientes afiliados manteniendo los lineamientos y estándares mínimos de seguridad preestablecidos previamente por la Super Intendencia de Bancos.

Sin embargo, ante la tendencia de ataques cibernéticos creciente es indispensable que se realicen análisis del estado de seguridad con el que se cuenta de manera periódica, y fomentar una cultura de seguridad que vaya a la par con las nuevas tecnologías, para así poder contrarrestar cualquier intento de vulnerabilidad de los datos.

Los análisis realizados a los niveles de seguridad de la banca arrojaron ciertas debilidades que pueden ser mejoradas con el fin de poner una barrera mas estrecha entre los datos que se manejan de los clientes en relación con los atacantes.

Para concluir, se espera que el banco siga poniendo en primer nivel a sus clientes con mantener la seguridad de sus datos y tome a buen recaudo las recomendaciones realizadas para así seguir siendo elegido por los mismos y recomendado.

REFERENCIA BIBLIOGRÁFICA

Antonio. (2016). *Banca Electronica contribuiciones a la Economia.* Ekos.

Carolin. (Abril de 2017). Avances Tecnologicos. *Ekos*.

Francisco, E. (2019). *Estudio tecnologico de avance Bancario.*

Karla, R. (2015). Protocolo de comunicación en la banca virtual.

Lux, M. (2017). El bien juridico protegido en los delitos informaticos . *Delitos informaticos*. Revista chilena de Derecho.

Moreno, A. (2017). Impacto de las vulnerabilidades ciberneticas . *PYMES*, pág. 15.

Orejuela, M. (2017). *Corresponsales bancarios como socio estratégico del sector financiero y facilitador en el aumento de niveles de bancarización.*

Pallasco, T. (2021). *Propuesta de mejora para la gestión de la seguridad informática del Banco Central del Ecuador, basado en el uso de pruebas PENTESTING* .

Perez, L. (2019). *E-Banking una necesidad de virtualizacion.* Guayaquil.

Piedra, C. (2019). Plataforma de Banca VIrtual y su implementacion. En *Masther thesis espol* (pág. 101).

Roberto, C. (s.f.). Delitos Financieros y economicos . *La revista del dercecho*, 33 .