La responsabilidad bancaria por fraudes electrónicos, en busca de la mejora para la entidad XY

Andrea Del Pilar Fernández Romero

Código 2501160

Universidad Militar Nueva Granada
Facultad de Ciencias Económicas
Dirección de Posgrados
Especialización Control Interno
Bogotá D.C
2020

Contenido

Lista de Graficas

RESUMEN

Este ensayo contiene una explicación de la responsabilidad de las entidades financieras, frente a los fraudes electrónicos, en donde se ven involucrados los clientes. En el mismo se describen fallos de la Corte Suprema en donde al finalizar el proceso le da la razón a los usuarios, explicando los motivos e impartiendo instrucciones para las entidades bancarias, en el mismo se exponen las circulares de la Superintendencia Financiera de Colombia, las cuales ha emitido para el control interno de estas organizaciones con el fin de proteger a los usuarios. Además se muestran las modalidades de fraude electrónico.

Para la elaboración del mismo se analizó la entidad financiera XY, revisando sus políticas de control interno frente al fraude y se formularon propuestas de mejora con el fin de mitigar las pérdidas económicas que han tenido por causa de estos fraudes.

Palabras clave: Entidad financiera, fraude, ciberseguridad, control, riesgos, pérdidas, control interno, modalidades de fraude, XY*

El nombre XY* es ficticio para fines académicos.

Abstract

This essay contains an explanation of the responsibility of financial institutions, in the face of electronic fraud, in which customers are involved. In it, rulings of the Supreme Court are described where at the end of the process it gives the reason to the users, explaining the reasons and giving instructions to the banking entities, in it the circulars of the Financial Superintendence of Colombia, the which has been issued for the internal control of these organizations in order to protect users. In addition, the modalities of electronic fraud are shown.

For its preparation, financial entity XY was analyzed, reviewing its internal control policies against fraud and proposals for improvement were formulated in order to mitigate the economic losses that they have suffered as a result of these frauds.

Keywords: Financial institution, fraud, cybersecurity, control, risks, losses, internal control, fraud modalities

INTRODUCCIÓN

Cada vez más se escucha que la tecnología ha llegado a nuestras vidas para quedarse, y que todos de una u otra forma terminaremos involucrados, si bien no la han presentado como un medio para mejorar y facilitar nuestras tareas, muchas veces no se menciona que la misma puede ocasionar daños y pérdidas económicas en muchos casos. Sin embargo esta ha logrado que sea el nivel de competencia de las organizaciones hoy en día, todas buscando implementar herramientas que faciliten su trabajo y la de sus clientes para lograr su fidelización y por su puesto nuevos usuarios.

Uno de los sectores más competitivos en cuanto a tecnología se refiere es el sector financiero, estos utilizan aplicaciones en las cuales se realizan todo tipo de transacciones, aperturas, inversiones y se analizan datos para créditos desembolsados en 10 minutos. Todo esto suena maravilloso, sin salir de tu casa puedes gestionar lo que necesites. Es en este caso es donde salen dudas, como saber si estas entidades garantizan que los datos que se ingresan a sus plataformas cuentan con la seguridad necesaria y no serán utilizados para otros fines, o que la información que el usuario registra en los portales sea la correcta, es decir que este en el portal autorizado y diseñado por la entidad financiera y no una página fraudulenta en donde estan robando mis datos personales.

Por lo anterior el ensayo analiza las diferentes regulaciones a las que las entidades financieras están expuestas, para garantizar la seguridad de sus portales, así mismo se explica los lineamientos que los entes de control exigen a las organizaciones, se citan ejemplos en los cuales las entidades asumen la pérdida por falta de control o insuficiencia de los mismos y se analizan diferentes clases de fraude electrónico.

Por último se analiza la entidad financiera XY*, en la cual se muestran sus políticas y manejos que se le dan a sus procesos internos, con el fin de ofrecerles estrategias para la mitigación de riesgos por fraudes electrónicos que han ocasionado pérdidas para la misma, estas recomendaciones se hacen basadas en los conocimientos, experiencias y formación que se ha adquirido en el transcurso de la especialización de Control Interno.

Formulación del problema

¿Cómo implementar estrategias de revisión en la entidad XY, que faciliten la tarea en los procesos por parte del auditor frente a la responsabilidad bancaria por fraudes electrónicos?

OBJETIVO GENERAL

Definir cuál es la responsabilidad bancaria por fraudes electrónicos para definir estrategias que sirvan para acompañar la labor del auditor, en la detección oportuna de las fallas en los procesos por fraude electrónico, que implican la responsabilidad de la entidad.

OBJETIVOS ESPECÍFICOS

- Identificar cual es la responsabilidad bancaria por fraudes electrónicos, incluyendo normatividad, lineamientos y casos probados.

- Analizar estrategias de mejora continua que faciliten la labor del auditor, en revisión de los diferentes procesos por fraude electrónico en la entidad XY.

La responsabilidad bancaria por fraudes electrónicos, en busca de la mejora para la entidad XY

La tecnología ha venido creciendo de forma exponencial los últimos 10 años, y este aumento se debe a las necesidades del mercado, o las de los seres humanos que cada día buscan facilitar nuevas tareas, que les permitan dedicar su tiempo en actividades que realmente le satisfagan. Por esto se habla que cada vez más las personas prefieren utilizar medios digitales para hacer sus pagos, comprar productos o adquirir nuevos de acuerdo a sus necesidades.

Todos los sectores económicos han tenido que adaptarse a nuevas realidades para ser competitivos, las industrias buscan mayor productividad a menores costos y el desarrollo tecnológico hace que este objetivo se cumpla.

Una de las industrias más grandes del mundo, el sistema bancario, tiene una oportunidad nunca antes vista, ser completamente digital y prestar sus servicios de una manera más eficiente, que llegue a muchas más personas y sectores económicos. Así como es una oportunidad, también representa un reto trascendental de cómo lograr que su sostenibilidad no se vea amenazada por riesgos inherentes de esta transformación.

Para Luis Humberto Ustariz González, autor de "Responsabilidad bancaria" "El sector financiero se encuentra en una metamorfosis del papel a la información digital" es decir que ese cambio que ha venido en aumento y que cada vez es más notorio se ha vuelto no solo en un nivel de competencia para las entidades del sector, si no en una política que las entidades ya adoptaron, una entidad que no se adapte a estos cambios con el tiempo va hacer absorbida por otra más grande, o simplemente puede llegar a desaparecer, pues no solo sus competidores se la llevarían, si no los consumidores, lo más probable es que se dirijan a entidades que les faciliten los procesos.

Según los últimos estudios realizados por OE, CÁMARA DE COMERCIO Y CNC el 90% de los internautas realizan algún tipo de comercio electrónico y de estos el 58% realiza estas búsquedas por su teléfono celular y utiliza diferentes medios de pago electrónico como PSE o tarjeta de crédito

(observatorioecommerce, s.f.)

Como se puede ver cada día la necesidad del mundo lo plantea, el uso de la tecnología llegó para quedarse y para sacarle provecho.

Sin embargo es fácil decirlo, pero debemos analizar cuáles son los verdaderos retos a los que se enfrentan las entidades para brindar mejores canales de servicios, que les permitan atraer nuevo usuarios y mantener los que ya tienen, productos que les brinden una mejor calidad de vida a los usuarios facilitándoles los servicios pero sobre todo que sean seguros.

Pensando en esta situación las empresas cada buscan implementar planes que les permitan generar una protección a sus canales virtuales minimizando los riesgos por Ciberataques o fallas en el sistema que afecten directamente a los usuarios.

A continuación menciono los actores principales para generar una mejora continua en los procesos de las entidades, las cuales deben contar como estándares mínimos para suplir estas necesidades e irlas actualizando:

- Equipo de trabajo: En este caso el recurso humano de cada entidad es fundamental, no solo por las funciones que le sean delegadas, sino que deben ser personas con una conducta moral buena, que permita generar confianza entre sus jefes, ya que la información a la que ellos pueden acceder, es la de cada persona, sus movimientos transaccionales, historia de crédito y demás.

- Comunicación: Acá se refiere a los diferentes canales que una entidad pueda llegar a tener en caso de fallas, o cualquier inconveniente que los usuarios puedan llegar a tener, el cual debe ser de acceso fácil y rápido tanto para las personas que lo están utilizando y que sirva de respaldo para que la entidad pueda actuar de forma inmediata.

- Notificaciones: Las entidades deben contar con un protocolo adecuado que permita tener actualizas sus bases de datos con información real de los usuarios, para poderles dar aviso los más rápido posible y de forma acertada en caso de llegar a requerirse.

- Contactos: En caso de que la entidad llegue a presentar alguna falla o un ataque a su sistema, es necesario que el personal o en caso de tener un Bot, cuente con una lista de contactos a los cuales se puede recurrir por las diferentes fallas, que permitan generar bloqueos y seguimiento, y más cuando estos servicios los prestan proveedores externos de la compañía. Además de estos es necesario en muchos casos notificar a las aseguradoras en caso de que aplique cuando suceda el evento.

- Planes de acción: Cuando ocurren estas falencias al sistema, las entidades deben tener certeza de que los aplicativos que están utilizando cuente con recuperación de información, y que estos principalmente garanticen que fueron probados antes de salir al mercado.

- Datos sensibles: Cuando se refiere a este tipo de información es la que cada persona deposita en cada solicitud, información personal y demás que sea requerida para cada tramite y que la entidad tenga bajo su custodia, es necesario saber en qué aplicativo y como se llega a ella en caso de ser solicitada por las aseguradoras o alguna entidad oficial que lo llegase a necesitar.

En este último punto es necesario hacer aclaración porque esta información es tan importante tenerla protegida, no solo por políticas internas o códigos de ética que cada entidad pueda llegar a manejar, si no que se encuentra protegida en el decreto 2555 de 2010 de la Superfinanciera, en el capítulo 7 libro 3, el cual menciona los deberes de estas entidades resaltado los valores de honestidad, idoneidad y sobre todo manejo de la información recibida. Estas entidades deben cumplir con todo el marco normativo para ellas y para los de los usuarios.

Para continuar con los datos sensibles, los cuales son de total reserva para la entidad, es necesario mencionar la ley 1581 de 2012, la cual nos habla de los datos personales de cada individuo y resalta en el Titulo II, que los datos que nos públicos no podrán estar disponibles libremente a no ser que los dueños de esta información lo decidan.

Con el decreto 2555 y la ley 1581 se pretender establecer un paréntesis en cuanto a la información que se recibe, ya que estos no solo ocasiona daño en las personas si no directamente en las entidades.

En cuanto al decreto 2555 de 2010 se adiciono circular jurídica en la cual resalta cuales son los requisitos mínimos para la seguridad y la ciberseguridad. Basados en los anteriores es necesario establecer y aclarar cuáles son entonces estas responsabilidades para fijar parámetros y estándares que permitan establecer mejoras continúan en las organizaciones.

Ciberseguridad

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio. (“Cisco”)

Según la adición en el capítulo V, nos habla de cuáles son los requisitos mínimos en cuanto ciberseguridad de la información se refiere para estas entidades, la cual comienza con que cada una de ellas debe establecer políticas, implantar procedimientos y así mismo contar con recursos físicos y humanos, encaminados a mitigar los riesgos asociados a la ciberseguridad, para esto el mismo anexo de la circular establece una serie de medidas como estándar básico para que las organizaciones se puedan guiar.

La más importante es que la política que la entidad elija este direccionada a la seguridad de la información y los riesgos asociados a la misma, esta debe ser aprobada por la junta directiva de cada entidad y todo debe estar debidamente documentado, es decir cuáles serían los responsables, los procesos de cada etapa y la gestión debe quedar al igual documentada en donde se evidencie claramente que hace a entidad en ciberseguridad.

En segundo lugar, las entidades deben contar una cultura que identifique sus principios y fomentar capacitaciones y difusión orientada a la ciberseguridad, y están se tiene que desarrollar periódicamente y contar con formación para el personal, sobre los riesgos a los cuales la entidad está implícita.

En cuanto al área de riesgos de cada entidad, la misma debe contar con canales de distribución de la información y la infraestructura necesaria para el desarrollo óptimo, en donde de acuerdo al volumen de clientes y las transacciones que se manejen por los canales virtuales, debe contar con evaluaciones de riesgos que le permitan tener una gestión eficiente, la misma no solo debe garantizar la seguridad de sus clientes, si no que se notifica a la junta directiva, en donde se les aclara e informa datos y estadísticas que pudiesen haber afectado la entidad la cual está dada para que se entregue semestralmente. Es de aclarar que la política y los lineamientos establecidos se deben estar actualizando de forma continua pues cada día las modalidades de ataque cambian.

El área de riesgos también queda como responsable de hacer verificaciones cuando se considere necesario y estar alineado con el cumplimiento de las políticas de seguridad de la entidad para que pueda dar el adecuado asesoramiento a la alta dirección y si aplica implementar nuevos controles o procedimientos como mejor estrategia.

Toda la información que la entidad tenga de ciberataque la misma debe ser reportada a la SFC, la cual debe contar con una descripción de los hechos y sobre todo cual fue el impacto que dejo en la organización, es decir como las pérdidas económicas, de la misma forma si es el caso, debe notificar si se vulnero algún dato de los usuarios que pueda llegar afectar a los mismo, finalmente debe entregar cuales fueron las medidas que se tomaron frente al caso para que no vuelva a ocurrir.

En el anexo de la SFC, menciona etapas para que las entidades puedan gestionar los ataques de Ciberseguridad:

- Prevención: las entidades deben priorizar la seguridad de sus plataformas, y por esto se establecen mecanismos que minimicen los impactos negativos hacia las mismas, empezado por tener controlado el acceso del personal interno que pudiese servir de puente para vulnerar algún control, en la prevención también se es necesaria una política interna que sea de directriz para identificar riesgos asociados y que determine una continuidad de la operación, en esta también la entidad debe estar dispuesta a dar la información necesaria que las autoridades llegasen a necesitar, y finalmente velar porque los consumidores estén informados sobre las políticas de seguridad con que se cuentan y brindar recomendaciones para los diferentes usuarios.

- Protección y Detección: Es necesario que cada entidad establezcas matrices de ocurrencias de posibles eventos, para que adelantarse a los diferentes eventos que llegaran a tener, y esto lo pueden hacer por diferentes procedimientos o nuevas estrategias de innovación que les permitan conocer cuáles son principales vulnerabilidades y hacer monitoreo de forma ágil y oportuna.

- Respuesta y Comunicación: En sus procedimientos la entidades deben tener claras cuales serán sus respuestas ante cualquier incidente que se llegase a presentar como lo son bloqueos, desconexiones u contraseñas como para mencionar algunos, así mismo en caso fallas a alguna plataforma debe contar con la infraestructura necesaria para revisar las demás plataformas ya asegurarse que no estén fallando las demás y en dado caso que lo daros vulnerados se puedan recuperar de forma rápida.

- Recuperación y Aprendizaje: Como se ha venido mencionando, cada entidad debe contar con la capacidad de recuperación y establecer planes de mejora que le permitan generar los planes preventivos y recuperación de las fallas a las que fue sometida.

Analizando el anexo y las circulares que sirven como directrices para estas entidades, las cuales deben cumplir y demostrar que si se está haciendo pues cada una de ellas está en la obligación de aplicarlas y darle a conocer, porque siguen ocurriendo casos en los cuales las mismas se ven afectadas y así mismo sus usuarios. La transformación que ha venido tendiendo el sector financiero hace que cada una de ellas se enfrente a nuevos retos, es acá donde es importante conocer cuáles son esas formas en que se puede llegar a presentar fraudes electrónicos, en donde se ven implicados tantos los usuarios como las mismas entidades.

A continuación lo que se pretende evidenciar es algunas de las comunes fallas y ataques de las cuales han sido víctimas las entidades y sus clientes, la idea es no solo mostrar ejemplos en Colombia si no algunos a nivel internacional con el fin de poder establecer algunas diferencias.

Phishing

Se puede considerar que una de las modalidades más conocidas es aquella que llama phishing, y en su definición se encuentra que es una forma de fraude en la cual las personas que lo practican que son llamadas phisher, obtienen de manera ilegal y no autorizadas por las personas, toda la información confidencial que le puedan extraer a sus víctimas, y estas lo hacen haciéndose pasar por entidades conocidas en donde las personas tienen algún vínculo para poderles generar confianza, es decir se hacen pasar como empleados de estas entidades y con habilidades personales logran extraer información de sus víctimas. El phising no es una palabra nueva, esta se hizo conocer en 1995, cuando un grupo de estafadores por medio de correos electrónicos atraían usuarios, haciéndose pasar con logos de la entidades y formatos parecidos como empleados de las mismas, en ingles esta viene

de la palabra pescar, es decir se asocia con la pesca de usuarios para ser estafados y esperar como se dice coloquialmente que estas muerdan el anzuelo, al hacerlo las personas entregaba de forma normal sus contraseñas o demás información requerida por estas personas. Además pescar en inglés es fishing, pero para este caso se le agrego la palabra "ph" porque es una sigla que se utiliza para los comúnmente llamados (hackers).

Cuando se empezaron a conocer estos casos, se dice que una de las primeras empresas que suplantaron o en la que se hicieron pasar por empleados fue la AOL "América Online" la cual era una empresa que prestaba servicios de internet, en este caso los phisher lograron extraer el código de programación de la página de ellos y crearon, una igual, al hacer esto también con el mismo código extrajeron información de sus clientes y empezaron a enviar correos con la pagina duplicada, para que los usuarios al ingresar revelaran información confidencial, esta fue de la primeras empresas conocidas que paso por este ataque de ciberseguridad.

Es de aclarar que esta modalidad ataca a las entidades conocidas que generen confianza y su principal característica es hacerlos por medio de correos electrónicos, con el fin que de lleven a los usuarios a las páginas que ellos crean para el robo de la información. De esta modalidad nacen diferentes maneras de fraude, otra de ellas es llamada Web Spoofing, en donde según el autor del libro lo describe de la siguiente manera

"Cuando un atacante elabora un sitio web impostor que luce similar al sitio web legítimo" (Ustariz, 2019, pp 125)

Es decir cada vez que las personas buscan la página de la entidad es posible que exista una similar para que las personas ingresen sus datos de manera voluntaria, usualmente a esta página le cambian alguna letra de su web original para que el leerla rápido, no se note que se está enviando a otra dirección.

Desde hace un par de años las navegadores también ha desarrollado medidas de seguridad para sus usuarios, sin embargo las nuevas modalidades han creado comando "JavaScript" el cual es un lenguaje de programación especial para estos navegadores, que lo que hace es descontrolar al navegador y lo direcciona a la página que ellos quieren, todo esto se hace internamente porque el usuario final no se da cuenta de estos cambios.

Pharming

Otra de las modalidades es el Pharming, que es muy parecida a la anterior mencionada el Spoofing, pero la diferencia entre las dos es que esta si no le cambia el sitio web original, es decir no altera letras ni números, si se compara la dirección es la misma, pero lo que hacen es que se direcciona al sitio web diferente. Esto aprovecha el funcionamiento de la red actual y en una dirección IP por parte de un servidor DNS para establecer la conexión y mostrarle al usuario lo que los estafadores quieren que mire para que tenga la plena confianza en dejar sus datos personales.

Las prácticas de pharming son una forma especialmente preocupante de cibercrimen, ya que el usuario afectado puede tener una computadora completamente libre de malware y aun así convertirse en una víctima. Incluso tomar medidas de precaución, como ingresar manualmente la dirección del sitio web o usar marcadores siempre confiables no basta, puesto que el desvío se produce después de que la computadora envía una solicitud de conexión.

Para prevenir esto lo primero que debe hacerse, es instalar una solución antimalware y antivirus potente, y adoptar prácticas informáticas sensatas, como evitar sitios web sospechosos y no hacer nunca clic en enlaces de correos electrónicos sospechosos.

Malware

Para hacer más fácil la aplicación de las modalidades anteriores, es muy utilizada la instalación de un malware el cual es un software malicioso programado para realizar diversas acciones en el computador del usuario o un servidor específico.

Por ejemplo un hacker puede instalar un virus o un troyano en la computadora de un usuario que cambia el archivo de hosts de la computadora para dirigir el tráfico fuera de su objetivo previsto, hacia un sitio web falso y de esta manera robar su identidad.

Para contextualizar un poco el funcionamiento de cada variante de Malware, los menciono a continuación.

Ransomware

Es la versión malware con la cual se secuestra el equipo y funciona bloqueando o denegando el acceso al dispositivo y su información personal hasta que pague un rescate al hacker.

Spyware

Busca información en un dispositivo o red para luego enviársela al atacante. Los hackers suelen utilizar spyware para conocer la actividad en Internet de un usuario y recopilar datos personales, como credenciales de ingreso, números de tarjeta de crédito o información financiera, con el propósito de cometer fraude o robo de identidad.

Gusanos o worms

Un gusano infecta un equipo y después se replica y se extiende a dispositivos adicionales. Algunos gusanos actúan como portadores de malware para instalarlos posteriormente. Otros están diseñados para reproducirse y volver lentas las conexiones de banda ancha de las redes,

Este puede llegar a infectar mediante la red a toda una compañía y afectarla gravemente.

Adware

Básicamente es publicidad no deseada, de la cual sacan provecho económico los creadores, por ejemplo los tipos comunes de adware son los juegos gratuitos y las barras de herramientas para el navegador.

Troyanos

Funcionan igual que los guerreros troyanos que ingresaron camuflados en un caballo de madera para destruir los muros enemigos. Inicialmente parece inofensivo pero Una vez instalado, el troyano se activa y, en ocasiones, llega incluso a descargar malware adicional.

Vishing

Si bien es de menor uso esta modalidad de fraude, esta consiste en enviar un mensaje de voz indicando que son entidades bancarias informando sobre problemas en su cuenta o tarjeta de crédito con el cual le solicitan los datos para corregir y así obtienen lo que necesitan para realizar los desfalcos.

La solución pasa por no hacer caso a los SMS que nos solicitan llamar o efectuar alguna otra operación ni dar datos por teléfono. Al igual que nunca hay que hacer click en un enlace que nos lleva supuestamente a la web del banco, tampoco hay que llamar a un teléfono aparentemente del servicio de atención al cliente.

Formjacking

Esta modalidad se da cuando servidores web infectados remueven la información de pago de los consumidores. De hecho, en promedio durante cada mes de 2018 más de 4.800 sitios web estuvieron comprometidos por un código de formjacking.

Tenemos en este momento plataformas de pago virtual como Mercado Pago, Amazon, Pse, que muchas de las industrias están utilizando para realizar sus transacciones comerciales, debido a esto, el Formjacking se convierte en una de las amenazas más latentes y que se debe prevenir enérgicamente.

Educación financiera

Dado lo anterior, las entidades bancarias podrían ir más allá de lo que la superintendencia financiera les indica acerca de Educación financiera, la cual consiste en dar claridad sobre los productos y el mercado general de los créditos a las personas para que así mismo tomen mejores decisiones y sus derechos no se vean maltratados.

También deben dar a conocer cada una de las recomendaciones y buenas prácticas para que no sean víctimas de algunas de las modalidades de fraude que describí anteriormente.

Por ejemplo, propongo que se les contextualiza sobre cada una de las modalidades, recomendar con expertos la prevención o identificación de los riesgos que conlleva hacer digitalmente los procesos bancarios e incluso sugerir o proveer software desde sus páginas para que las personas los usen y estén seguros en sus transacciones.

El banco XYZ por ejemplo tiene un programa que previene varias de las más comunes suplantaciones, se encuentra en su página web, una vez el usuario ingresa a su cuenta arroja una ventana emergente sugiriendo la descarga del software que ayuda a prevenir amenazas en internet.

Si bien esto denota un desgaste adicional se puede compensar con reducción en las reclamaciones que los clientes hagan por fraudes sobre sus productos bancarios.

Otro mecanismo muy utilizado es la utilización de teclados numéricos cifrados que el cliente ubica fácilmente y bloquea cualquier ataque de robo de información. También promueven el uso de antivirus para prevenir la infección de malware común.

Responsabilidad Jurídica en los Fraudes electrónicos

Lo anterior tiene una doble connotación, tanto la seguridad como el servicio que está dispuesta a asumir la entidad financiera, por un lado busca que sus procesos sean seguros dentro de su autonomía comercial y por otro lado vender el concepto de seguridad que tanto gusta en las personas por el hecho fundamental de que lo que está en juego es su dinero.

De igual manera, cumpliendo su rol, la superintendencia financiera da unas instrucciones a través de las circulares 052 de 2007 por la cual Imparte instrucciones relacionadas con los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios., 022 de 2010 042 2012 y 049 de 2016 en las cuales vale la pena resaltar que el fin de la misma, es que estas organizaciones establezcan diferentes mecanismos que permitan tener calidad en sus procesos de seguridad y que estos tengan la información clara y necesaria para cualquier usuario el cualquier plataforma, es decir ya sea que la busque por dispositivos móviles o paginas registradas de las entidades.

Vale la pena aclarar que todo lo dispuesto en esta circular es de carácter obligatorio, es decir las que estén en vigilancia por la Superintendencia Financiera de Colombia, la debe adaptar a su organización con algunas excepciones como lo cita en su libro (Ustariz, 2019), “La SFC da como excepción de la circulas a las entidades FOGAFIN, FNG, FOGACOOP, entre otras” (p.140), con esto no quiere decir que las no estén obligadas a cumplir con la circular no requieran cumplir con los requisitos de seguridad, pues todas están entidades deben garantizar que sus sistemas se les hacen pruebas de seguridad periódicamente que beneficien a las entidades y los usuarios y sobre todo que los mismos sean confiables demostrando una mejora continua en los mismos. En este punto las entidades son libres de usar diferentes programas o

herramientas para la realización de las pruebas, así mismo de fijar sus políticas y procedimientos para garantizar su adecuado funcionamiento.

De otra parte en la circular también da instrucciones claras en donde las entidades deben salvaguardar la información de todos sus clientes a través de sus diferentes canales, la misma se encarga de abarcar todos los parámetros necesarios, es decir tecnológicos, y de procesos para que las entidades no tenga excusa para seguir los lineamientos.

Para cada modalidad y en las que más se utiliza el fraude, la circular aclara aspectos relevantes en el fraude electrónico, uno de ellos son los cajeros automáticos en donde las organizaciones debe contar cámaras de seguridad, información cifrada, contar con canales de autenticación al igual que seguridad física que impida que terceros accedan a la información. Para los canales de internet SFC, establece que cada portal tenga códigos internos de algoritmos, que están blindados ante cualquier ciberataque y que siempre las entidades están realizando pruebas de sus portales.

Los dos anteriores son solo dos ejemplos que la circular cita para que las entidades puedan comprender que la finalidad de ellas es la protección de los consumidores, que sus canales deben contar con todas las medidas necesarias, no solo las que se encuentren de carácter obligatorio si no las que las mismas organizaciones puedan llegar a establecer. Porque es responsabilidad de ellas que se vulnere su seguridad.

Por lo anterior, por esta responsabilidad que deben tener las entidades, es importante señalar que la Corte suprema de Justicia el 19 de diciembre de 2016, señalo un caso en donde una entidad financiera**,** se vio afectada por un fraude electrónico bajo la modalidad ya explicada phishing. Uno de sus clientes le fue sacado de su cuenta de ahorros 124 millones, lo más grave es que cuando el cliente reportó a la entidad que la página le salía un mensaje de error, pero la misma de acuerdo a los expuestos por los funcionarios no fue considerada como grave, pues en ocasiones se desconectaba del servidor y la página enviada por el cliente tenía el mismo dominio, pero fue en ese momento cuando los delincuentes aprovecharon que el cliente accedió a la misma y accedieron a sus claves

La corte en su análisis quiso indagar y demostrar cual es la importancia que le dan están entidades a la calidad en seguridad, según lo expuesto en la sentencia del 19 de diciembre de 2019 expediente 05001-31-03-001-2008-00312-01

“señala que las entidades deben reparar perjuicios ocasionados por fraudes electrónicos y deben asumir la responsabilidad por la defraudación sufrida por los usuarios a través de transacciones electrónicas”.

Con esto también se demuestra la gran responsabilidad de las organizaciones por crear mecanismos y herramientas que fortalezcan sus controles de seguridad y brinden barreras a todas sus plataformas, enfocadas en el beneficio de los usuarios.

Además en el mismo análisis la Corte Suprema señaló la importancia de los riesgos asociados a esta práctica, menciona que las mismas deben tener claro cuáles son los que más afectan la

operación y establecer cómo los van a mitigar, pues en el mercado financiero donde siempre hay cambios es necesario estén en constante alerta y conocimiento para mejorar, pues en dado caso en que las entidades no pueden cumplir con mecanismos de seguridad o no sean suficientes tendrán que ser responsables y asumir los costos de las mismas, es decir las entidades que utilizar todas las plataformas tecnológicas, tendrán que estar en constante alerta y garantizar que hacen hasta los procesos más rigurosos para poder suplir las necesidades de seguridad, crear alertar, y proteger siempre sus clientes.

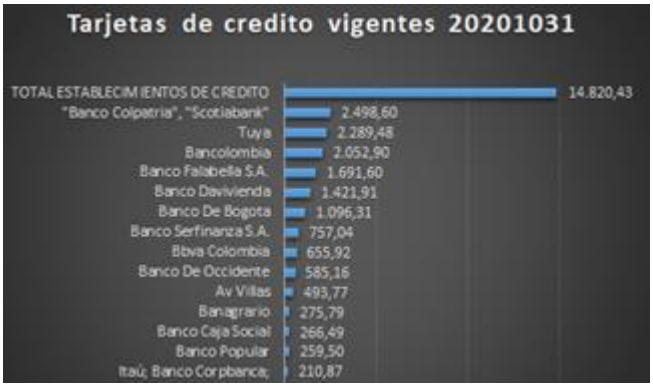
Para cada modalidad de robo electrónico en el que la entidad tenga la responsabilidad, la Corte Suprema en la misma sentencia, señaló algunos parámetros en los que se pudiera llegar a presentar fraude, diferentes a los canales de internet o celular, pero que involucran su tecnología:

- Suplantación de un tercero: Cuando otra persona abre una cuenta de ahorros o corriente, con los datos de otra persona el suplantado. La entidad financiera está en la obligación de investigar la documentación presentada, y de pasar por los filtros de seguridad que la entidad estableció, para evitar fraude.

- Traslado Fraudulento: En este se trae a colación el caso de un municipio que se percató del traslado de dinero de una cuenta a otra en la misma entidad, en donde se demostró según (Expediente 68081-3103-2002-00025-01 OP. Cit,. Pp29) que la entidad financiera no cumplió con los protocolos de seguridad y permitir la creación de una empresa que le permitiera hacer traslados entre dos empresas diferentes.

Finalmente la corte también cito la Circular 029 de 2014 en donde se establece que a los consumidores se les deben crear diferentes herramientas que cumplan con toda la seguridad en donde ellos puedan realizar transacciones entre sus productos o a otras entidades, también debe ofrecer diferentes posibilidades de manejar sus contraseñas, elaborar cuáles serán los procedimientos y buenas prácticas de bloqueo, así como los perfiles de cada cliente, es decir cuáles son sus costumbres en donde realiza sus operaciones habitualmente, para que permitan generar alertas a las entidades y evitar fraudes.

Ahora, se ha descrito los fraudes que ocurren en su mayoría por traslados de cuentas de ahorros o corrientes, y se han señalado algunos ejemplos que la Corte Suprema ha señalado con distintas ópticas y recomendaciones para garantizar la seguridad de los usuarios, sin embargo nos queda uno de los fraudes más conocidos, el de las tarjetas de crédito, pues desde hace años estas se crearon en Estados Unidos alrededor de los años 20 siendo los hoteles unos los pioneros en permitir la utilización de las mismas y su creación se le atribuye al National Bank de Brookling, en Colombia desde el año 1962, se empezó con la utilización de las tarjetas, hasta el momento según informe de la superintendencia financiera de Colombia existen catorce mil tarjetas vigentes, como se muestra a continuación:



Gráfica 1 Tarjetas de Crédito vigentes

Elaboración fuente propia

Con esto lo que se pretende evidenciar es que uno de los medios de pagos más utilizados y ha venido creciendo en los últimos años por múltiples factores, entre ellos por la competencias en tasas, facilidad de cupo, algunas cuentan con utilización internacional, entre otros. Según Ustariz pag 157,"El ranking de tarjetas lo lidera Costa Rica, llegando al 22.4% del PIB", seguido por Brasil y Chile.

Sin embargo cabe resaltar que las mismas deben contar con los mismos requisitos de seguridad y calidad para brindarles a los usuarios la protección en su utilización. Estas deben contar con un proceso de autenticación en donde el banco debe contar con mecanismos que le brinden información sobre el consumidor y el establecimiento en donde está realizando la compra, también debe contar con las medidas de seguridad que permitan tener confidencialidad entre las partes que estén realizado el procedimiento, en este último punto es de aclarar que los usuario también están en la obligación de cuidar sus datos y no dar a terceros los datos de seguridad de las tarjetas, de esta manera las entidades también elaboran perfiles de cada usuarios donde conoce las tendencias de compras, y si es el caso bloquea la transacción y puede llegar a verificarla directamente con el usuario antes de realizar su compra.

La Súper Financiera de Colombia en capítulo 1 numeral 5 de la circular básica, señala algunas obligaciones específicas que deben tener las entidades financieras para el manejo de las mismas:

- Los cupos otorgados a los usuarios deben estar documentados en las políticas de cada entidad, de acuerdo a los perfiles de riesgos que las mismas manejan y deben estar acorde con el sistema de administración de riesgos.

- Cada entidad evaluará de forma segura el aumento de los cupos de cada cliente de acuerdo a sus niveles de riesgos.

- En la circular se destaca practicas inseguras que las entidades deben tener en cuenta, como lo es el ofrecimiento de cupos sin aceptación del cliente, también ofrecer más cupo sin hacer los estudios de riesgos, faltar a las políticas de la misma entidad por cupos excesivos, realizar cobros no descritos o no informados a los usuarios

- En los convenios que las entidades realizan con diferentes establecimientos, informarles que los mismos están en la obligación de verificar la tarjeta con el documento de identidad como lo señala la circular.

Finalmente en la circular se refleja que el uso de las tarjetas de crédito, deben tener seguridad tanto por parte de la entidad como por parte del usuario, y que es importante que al momento de la entrega las entidades informen y capaciten el uso de las mismas y el debido cuidado al momento de su uso, ya sea en transacciones físicas o en compras por internet, sin liberar a las entidades de su responsabilidad en los casos a lo que haya lugar y se compruebe que el usuario le dio el correcto manejo, estás estaría en la obligación de respaldar cualquier evento de fraude.

Para cada entidad es importante dar solución oportuna a sus fallas y estar en continuo desarrollos de plataformas tecnológicas que les ayuden a mitigar riesgos y realizar los controles preventivos, en todos los productos que ofrecen y que puedan generar ataques de ciberseguridad, pues este tema se ha convertido a nivel mundial en investigación y en estar buscando mejoras que permitan adelantarse a los delincuentes, en Colombia por ejemplo desde el 2011 se ha venido trabajando en diferentes políticas de Ciberseguridad, la cual dio lugar a un ataque recibido en el 2011 donde dejó sin servicio a portales públicos.

Con los anterior se puede concluir que el uso de herramientas y políticas de seguridad es necesario para cualquier entidad que pretenda utilizar diferentes portales y la tecnología necesaria para beneficio propio y el de sus clientes, por esta razón en diferentes ocasiones la Superintendencia Financiera de Colombia ha señalado buenas prácticas, deberes y obligaciones que son de obligatorio cumplimientos para estas entidades como lo demostró la Corte Suprema en donde plasmo en diferentes escenarios que las entidades que evadan los controles o en dado caso se demuestre que estos no fueron suficientes, deberán asumir los costos de los fraudes y responderles según cada caso a los clientes que fueron víctimas y demostrar cuáles son sus planes de acción que mitiguen los riesgos materializados.

Fundamentalmente todo lo plasmado anteriormente se ha convertido en un verdadero reto para estas entidades, pues no solo tiene que establecer controles y seguimientos continuos, si no tratar de ir más allá de los delincuentes, incluso según un estudio realizado por asobancaria en el 2019, nos revela que existe cooperación internacional para lucha contra los ataques cibernéticos a las entidades financieras, en donde lo que se pretende en que entre varios países se unan para buscar mejores estrategias y buenas prácticas que adopten las de más que sean de fácil aplicación y de ejemplo para los demás que deseen aplicarlas, esta unión creó un grupo llamado el CEG, siglas en inglés que traducen grupo de expertos cibernéticos que se enfatiza en los riesgos y en la manera de buscar estrategias que se puedan aplicar a través de pruebas basadas en las diferentes amenazas que han logrado identificar, el grupo también ha establecido una serie de lineamientos aplicados de forma internacional los cuales consisten en:

- Marco de Ciberseguridad: Establecer cuáles son las normas que se adaptan a cada país y de esta forma plantear los riesgos.

- Gobernanza: Mediante políticas, las entidades deben establecer cuales son los verdaderos responsables de los procesos, y asegurarse que los mismo cuenten con los recursos físicos y tecnológicos que llegarán a recurrir.

- Evaluación de riesgos: Las entidades debe establecer y priorizar los riesgos, para poder desarrollar programas que los mitiguen.

- Seguimiento: Realiza pruebas periódicas, no solo a sus procesos internos si no a las redes que utilizan.

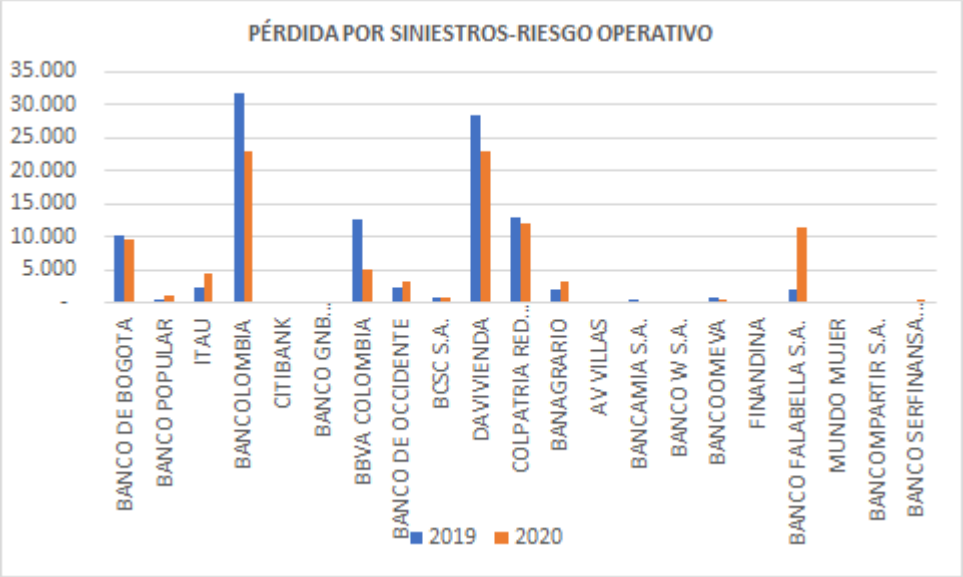
- Respuesta: Aca es donde cada una debe tener una capacidad de respuesta rápida y evaluar cual es el impacto de la misma

- Recuperación: Después de cualquier falla la meta está en la recuperación rápida y oportuna, con el fin de eliminar de raíz los problemas y generar controles específicos.

- Aprendizaje continuo: Todos los anteriores lineamientos se basan en aprender de los errores y que cada entidad promueva el mejoramiento de cada proceso.

Como podemos evidenciar todos los esfuerzos están unidos, ahora nos queda evidenciar cómo en Colombia ha venido creciendo las denuncias por fraude, según un artículo publicado por el tiemp**o,** indica que el primer semestre de este año, las denuncias por fraude electrónico aumentaron en un 59%, en donde señala que los medios utilizados para los mismo fue PSE, los portales de diferentes entidades bancarias y banca móvil.

Al hacer un análisis de las pérdidas por fraude según los estados financieros reportados por la Superintendencia Financiera de Colombia, al corte de agosto del 2020 las pérdidas por fraudes en las entidades financieras continúan, como se muestra en la siguiente gráfica en la cual se compara este año versus el anterior.



Gráfica 2 Perdida por sinisestros

Elaboración fuente propia

Por lo anterior se analizará la entidad financiera XY, con el fin de establecer cuáles son los controles que aplica actualmente, cómo ha impactado sus resultados, y cuales son estrategias para la mitigación de los mismos, este se empezará con el conocimiento de las políticas con el fin de establecer, cuáles serían las mejores prácticas que puede adoptar el equipo de control interno.

Analizando las políticas de la entidad XY se puede encontrar que la mismas cumplen con las condiciones y lineamientos dadas por la Superintendencia Financiera de Colombia, entre las cuales encontramos la de garantizar las operaciones y tecnología para sus clientes, en la cual busca dar soporte a los incidentes y las peticiones, además de asignar responsables que brinden soluciones oportunas en los tiempos acordados y con la calidad esperada por la entidad, además buscar priorizar requerimientos según su grado de importancia, teniendo como soporte una mesa de servicio para pronta solución y optimización de tiempo y respuesta. Para el desarrollo de la política la entidad cuenta con un monitoreo automático, el cual hace una revisión previa, después de esto busca identificar cuáles son los proveedores o los aliados par el registro de los incidentes, al finalizar este monitoreo el gestor de incidentes analiza el caso, identifica las fallas y le da una calificación del riesgo, es decir si es bajo, medio o alto y trata de dar solución inmediata si aplica o de lo contrario escala el caso. Todo esto ocurre en tiempos muy rápidos, lo cual permite buscar soluciones en un primer nivel a los clientes, o de los contrario escala a las personas indicadas según el proceso, es de aclarar que todos esto debe quedar documentado, el sistema envía un reporte de los monitoreos automáticos y posteriormente las personas que recibieron y gestionaron los casos lo deben hacer.

Como solución a la misma en caso de fallos en el proceso o en el sistema, se debe entregar la evidencia de las fallas al laboratorio de pruebas para que pueda identificar cuál fue el origen del problema, hacer pruebas y certificar cuál fue la solución técnica, para quede documentada

en el proceso de mejora continua. Al cierre de cada incidente, también se le asigna una calificación de criticidad para analizar el impacto.

Otra de las políticas de ciberseguridad de la entidad XY, es la contingencia Tecnológica, la cual busca crear ejercicios que se anticipen a daños en el sistema, estos se deben hacer y certificar por lo menos una vez al año o en su defecto cada vez que se presenten cambios que puedan llegar a impactar la infraestructura tecnológica de la entidad. Además esto aplica no solo para los procesos internos, si no para los proveedores los cuales al momento de la contratación deben certificar que cuentan con planes de contingencia, lo más importante de esta clase de eventos es que garanticen la misma funcionalidad en el ambiente normal de producción y en el de pruebas. En el desarrollo se plantea que se deben hacer una vez al año, definir y priorizar fechas para dichos ejercicios, contar con evaluaciones de riesgos y cuáles serán sus estrategias de gestión, así como llevar el control de los tiempos reales de cada actividad todo debidamente documentado y divulgado a todo el equipo de tecnología.

El objetivo de la política descrita anterior es que se pueda controlar y ejecutar los procedimientos que puedan llegar a soportar todas las operaciones de tecnología y administración de infraestructura de cómputo de la entidad XY, para esta también nombra como dueños del proceso a las vicepresidencia de infraestructura, quien también es la encargada de garantizar que los proveedores cumplan con las condiciones de calidad establecidas, además esta vicepresidencia se encargará de toda la operación diaria, la actualización de la documentación y el monitoreo y supervisión del mismo.

Política de la administración de datos, la cual tiene como objetivo mantener la integridad, verificar la disponibilidad y la confidencialidad de los datos que se encuentran en la infraestructura tecnológica de la entidad, en esta el proceso debe tener indicadores de desempeño, contar con condiciones que respalden la infraestructura , realizar gestión y seguimiento a la misma, este también debe estar respaldados por manuales que cumplan con el sistema de administración de riesgos y con las circulares que impacten al proceso dadas por la Superintendencia Financiera de Colombia.

En la política de rol de servicios tecnológicos, se deben crear condiciones de soporte, las cuales deben estar respaldadas bajo acuerdos operativos internos y de proveedores, estos deben ser aprobados por los directores de la entidad, y cualquier actualización que se haga, debe ser autorizada por los mismos, para el caso de los proveedores, estos también evaluaran si cumplen o no con las condiciones de calidad establecidas, es de aclarar que cada año se debe entregar un informe de los controles que se hicieron y las fallas encontradas, para el caso de los proveedores, deben contar con un registro en donde se especifiquen los paquetes de los servicios que presten informando cuál es su parametrización y configuración, información documentada en manuales. En caso de encontrar fallas, al igual que en las anteriores políticas se priorizan según su grado de criticidad, se gestionan y documentan las acciones ejecutadas, con el fin de minimizar riesgos, además según el caso se escala para mejores soluciones.

Se ha hablado de la priorización de riesgos en la que cada área los debe identificar y darle una calificación, pero para estos la entidad cuenta con un procedimiento el cual busca una

estandarización, entre ellos encontramos como primera instancia, revisar la herramienta donde se registran las incidencias según la prioridad establecida por cada área, se debe hacer una análisis con los registros anteriores para encontrar si hay soluciones que se puedan adoptar con el fin de dar solución y disminuir la criticidad, en caso de que no se pueda dar una solución oportuna se asigna a un responsable para que de la solución e identifique el problema de raíz, con esto también se verifican cuales pueden se las vulnerabilidades a las que la entidad XY está expuesta, en caso de encontrar alguna existe un equipo transversal de calidad que también documenta las mismas. Para el envío de estas la entidad cuenta con Site en donde por medio de formulario, se envían y se gestionan, lo primero que se debe hacer es ingresar, el área emite un concepto, anexa la documentación de evidencia que llegase a tener y las pasa al laboratorio de pruebas en donde la finalidad es darle solución al problema.

El gestor de soluciones de la entidad XY, lo primero que debe hacer es validar las actividades enviadas para darles solución, en lo posible erradicar el problema, documentar en forma detallada el resultado del análisis, revisar las acciones ejecutadas si aplica verificar y ajustar los procedimientos de acuerdo con los criterios de la entidad.

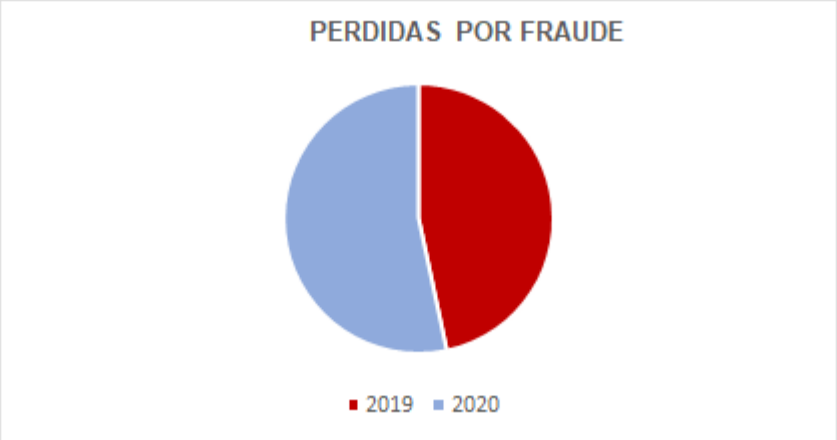
En cuanto a la política de la prevención del fraude, está enfocada a garantizar la operación de los clientes de forma segura y con calidad, en este proceso se articula las etapas del ciclo de fraude las cuales son disuasión, detección, mitigación, análisis, investigación y judicialización las cuales son establecidas por el gobierno de riesgo de fraude, este básicamente se reúne para definir las estrategias antifraude de la entidad, y evalúa procesos de autenticación, verificación y seguridad digital, este también debe justificar los riesgos que estableció, sus impactos y si aplica una validación jurídica. El comité debe documentar y atender recomendaciones, impartir instrucciones e informar a los grupos impactados de acuerdo a los procedimientos vigentes de cada proceso.

En caso de que en la entidad alguna área, tenga una propuesta para el comité, esta será recibida por la línea de negocio, la cual después de su análisis identificara los focos de fraude y riesgos de la misma, en caso de ser aprobada se establecen responsables y se actualizan las matrices de la entidad.

La entidad también cuenta con un departamento de modelos analíticos de fraude, el cual es el encargado de replicar modelos existentes que generen buenas prácticas, validar modelos estadísticos, realizar indicadores de precisión, construir variables, programar modelos documentarlo, revisar las especificaciones su alcance e impacto, todo estos estudios tienen como fin evaluar la confiabilidad de los modelos con que la entidad cuenta, esto se hace de forma periódica, que también sirven para identificar fallas o problema de desactualización. Este departamento al realizar estos modelos lo primero que hace es identificar el propósito y objetivo del estudio, identificar los datos a estudiar, evalúa costos, disponibilidad, licencias, almacenamiento y accesibilidad, integra datos, consolida, estandariza y crea informes detallados que sean de ayuda para la entidad.

Cuando se trata de estudios de fraude presentados por proveedores de la entidad, estos deben cumplir con características especiales como los son, estadísticas, análisis de datos, planes de mejora continua y sobre todo que se garantice el adecuado control y calidad de sus procesos.

Con estas políticas la entidad buscar crear filtros que minimicen los riesgos de seguridad para prestar un mejor servicio a su clientes y dar disposición a las circulares, que los rigen, la entidad en las políticas analizadas también busca la mejora continua y el desarrollo de nuevos modelos que se adapten a la misión de la misma. Sin embargo a pesar de las mismas las cuales son de lineamiento y directrices claras, la entidad ha presentado fallas en sus aplicaciones tecnológicas, las cuales al corte de Septiembre del 2020 ha generado pérdidas, por fraude transaccional, incluso en comparación con el año anterior, como se muestra a continuación:



Gráfica 3 Perdidas por Fraude

Elaboración fuente propia

Según la información presentada la misma ha perdido en lo corrido del año alrededor de treinta y dos mil millones de pesos después de los pagos de seguros, cifra que superó las del año anterior, la cual para el mismo corte era de veintiocho mil millones, además se pudo investigar que los fraudes electrónicos de la entidad en un 49% corresponden a la modalidad de Phishing, las demás eran por tarjetas de crédito en los cuales no se pudo demostrar que los usuarios tenían responsabilidad alguna y otras modalidades de fraude no electrónicas como fallas en los cajeros automáticos.

Cabe anotar que este año ha contado con una contingencia no esperada, y que las personas se vieron obligadas a utilizar los canales virtuales el fraude por estos canales ha crecido en un 59%, como se ha venido mencionando, lo que hace que las entidades financieras tengan que buscar nuevas estrategias que mitiguen los riesgos de vulneración de sus entidades. En la entidad XY se analizaron las políticas de fraude y riesgo con las que cuenta, evidenciando que no solo con estas, se solucionan los filtros de información.

Es por esto que se hace necesario ir más allá y revisar como son los controles del área de control interno con el fin de establecer estrategias para la entidad que se anticipen y que se convierta en un control preventivo eficiente que colabore con la mitigación de las fallas en los procesos de fraude.

El objetivo del proceso de la entidad XY, es asegurar que se cumplan las políticas, las normas tanto internas como externas, así mismo que se puedan identificar las omisiones, fallas, pérdidas, y a las oportunidades de los procesos, todo esto con el fin de ayudar a la organización a cumplir con los objetivos propuestos, enfocados en una estrategia sistemática y disciplinada que permita la evaluación y mejora eficiente de la gestión de riesgos, control y gobierno, además de proponer acciones de mejora, preventivas y correctivas, y si es el caso que se pueda incluir las actividades de consultoría.

El proceso mencionado comienza con la elaboración del plan anual de auditoría, el cual se hace ante la junta directiva y basada el código de ética de auditoría interna de la ISO – 9001:2015, la cual trata del sistema de calidad y sus mejoras, además de las circulares de la Superintendencia de Sociedades a las que haya lugar.

Para la entidad XY, se aplican las siguientes políticas para el área de control interno. Comenzando por la estructura del área, la cual se encuentra adscrita a la junta directiva, a través de un comité de auditoría, este es el encargado de prestar servicios de aseguramiento y consultoría, y lo hace por evaluaciones independientes y objetivas, en esta se enfoca en la labor del área como sistemática y disciplinaria generando valor y lo más importante contribuyendo al logro de los objetivos de la entidad XY. Así mismo esta deberá desempeñar sus funciones acordadas por el gobierno corporativo y el estatuto de auditoría interna el cual es el que los rige.

En cuanto al modelo que se utilizara de evaluación para el sistema de control interno, deberá ser exclusivo para la entidad y debe estar definido y dirigido desde la auditoría interna. Así mismo como menciono deberá elaborar su plan anual de auditoría, en el cual deberá priorizar de acuerdo a los niveles de exposición de riesgo de la entidad y deberá satisfacer los requerimientos de los entes de vigilancia externos e internos, el plan para la entidad XY, se presenta al comité de auditoría a más tardar en el primer comité del año para su aprobación. Para que se pueda ejecutar el plan, la administración de la entidad, será la encargada de proveer los recursos humanos, económicos, técnicos y de capacitación necesaria para que se pueda contar y estructurar el equipo de trabajo, el cual será especializado y certificado acorde a las políticas y estándares que puedan ser aplicables al ejercicio de auditoría interna.

Cabe aclarar que por casos especiales que la junta o presidencia requieran, podrán solicitar auditorías que no estén incluidas en el plan de anual entregado o también podrán ser solicitadas como consultores de algún proyecto importante que se requiera. Sin embargo, en su rol de auditores, estos no podrán desarrollar o asumir funciones operativas o administrativas que llegasen a comprometer su objetividad o independencia.

El área administrativa de la entidad XY, también se encargará de la ejecución y mantenimiento del sistema de control interno y lo que lo componen, y entraran dentro del presupuesto del área los costos por capacitación, está definido para que sea de 40 horas anuales para los auditores, es de aclarar que para las personas que se vinculen como nuevas, estas ya deben contar con certificaciones y evidencias de su formación profesional como auditores internos.

En la etapa de planeación de la auditoría, la entidad contempla que en su elaboración, se deben tener en cuenta las expectativas de la alta gerencia y por supuesto la del comité de auditoría, quien es la encargada de determinar el universo auditar, durante la misma se busca que el plan se desarrolle siempre pensado en la eficiencia, que estén soportadas por la tecnología y los principios de autocontrol, autogestión, y autorregulación, además las actividades en la entidad XY, se sincronizan con las demás áreas de relación como revisoría fiscal, u otras de riesgo. De igual forma si durante su desarrollo se requiere algún cambio en el plan de auditoría la entidad señala que siempre que esté aprobada por el comité, no habrá problemas para cambios, desde que cumplan con las condiciones mínimas para ser tenidas en cuenta. como lo son evaluación del riesgo, la capacidad instalada y la disponible, además del presupuesto que se tenga aprobado por dependencia, los recursos asignados, tanto físicos como humanos, las obligaciones normativas y por último los acuerdos internos en el flujo de la operación.

En el desarrollo de la planeación del plan de trabajo, la entidad XY, resalta que en los casos que exista conflicto de interés para las auditorias asignadas, se deberán informar a los jefes, antes del inicio del trabajo. Además contempla que cuando ya se esté en el proceso de auditoría y si aplica, se debe considerar las expectativas del auditado y se hará una evaluación de la gestión del riesgo del proceso, en este caso la entidad manifiesta que la primera línea de defensa serán los dueños del proceso y menciona que las segundas líneas de defensa son las áreas de riesgo, el auditor desarrollará el plan de acuerdo con el cronograma establecido.

En la ejecución del trabajo de auditoría para entidad XY, se pudo establecer que se enfoca en que la misma se centre en el cumplimiento de los objetivos y el alcance establecido, además dentro de los lineamientos también se menciona que los auditores deben cumplir con la ejecución del trabajo teniendo en cuenta la debida prudencia, competencia y debido cuidado profesional, cuando el auditor lo considere deberá aplicar un procedimiento de selección de muestra que considere el más adecuado, así mismo para la entidad es importante aclarar que en el desarrollo de trabajo se pueden presentar eventos que generen desviaciones al cronograma planteado, por casos especiales o proceso que lleven más tiempo, cuando esto suceda aclara que lo único no puede considerar admisible es que se modifique el objetivo y el alcance del trabajo, en caso de que lleguen a presentarse se debe reportar al jefe inmediato y este ya determinará que acción se puede seguir.

Para la entidad XY, es importante contar con auditorias de calidad, incluso señala que si es el caso, se podrá contratar personal especializado siempre y cuando cumpla con la aprobación del comité de auditoría, en la busca de la calidad la organización también busca que la información que los auditores vayan a incluir en los papeles de trabajo debe ser precisa, concreta que sea clara y sobre todo sea elaborada técnicamente, además los mismo deben llevar unas conclusiones objetivas que contribuyan a la toma de decisiones, y mejora continua pues estos

también deben ser archivados, no solo para soporte del trabajo o si algún ente externo lo llegase a necesitar, sino como muestra de mejora para los demás procesos que aplique. Además no solo deben contar con los papeles ya mencionados, sino que después de cada ejercicio se debe presentar un informe final, el cual debe contener hallazgos si hay lugar, las prácticas que se utilizaron y las recomendaciones.

En este último para la organización es importante que las recomendaciones y las conclusiones que salgan después de cada proceso de auditoría, se discutan con los usuarios responsables del proceso auditado y se debe hacer antes de emitir el informe final. Para la aprobación de estos se debe asegurar que los mismos lleguen a las personas que se encuentran en disposición de adoptar las medidas correctivas o las que puedan asegurar que tomen las medidas o planes necesarios, según sea el caso y cada informe debe contar un consecutivo para su fácil acceso y no puede ser emitido sin la autorización del jefe del área, acá la organización permite que en el mismo se puedan incluir párrafos de confiabilidad y limitación de la distribución, es de aclarar que dependiendo de cada proceso aplica lo mencionado anteriormente, pues la organización cuenta con información y cifras que no pueden ser divulgadas a no ser que sea en solicitud por un ente de vigilancia externo.

La entidad XY, menciona que se debe realizar su respectivo seguimiento después de cada labor de auditoría, es decir por ejemplo cuando se presentan hallazgos, se espera una acción inmediata por parte de la dirección a cargo y debe ser monitoreado hasta que se le pueda dar la solución definitiva a lo encontrado, posteriormente también se podrán emitir recomendaciones y una revisión periódica para verificar el cumplimiento de la mejora, y todo esto debe ser entregado y evidenciado en los informes. Esto también aplica para las consultorías externas que se presenten en casos especiales, deberán cumplir con los mismos lineamientos establecidos, tanto en desarrollo de su trabajo como en la calidad de los informes.

Al igual se pudo verificar que en las políticas los casos que lleguen por fraude, no se estudian por el área de control interno, si no que estos son analizados por entes externos quienes se encargan de las respectivas evaluaciones de los casos, para entregar del informe final, y evidencia de los mismos., con el fin de que la entidad pueda aplicar las mejoras necesarias a sus procesos.

Dado lo anterior se busca dar a conocer estrategias para el área de control interno de la entidad XY, que puedan brindar un asesoramiento desde su rol, basados en las normas internacionales para el ejercicio profesional de la auditoría interna, empezando en el capítulo V, el cual nos habla de aptitud, en la cual no solo se refiere a las habilidades que pueda llegar a tener cada miembro del equipo, sino también a la posibilidad de asesoramiento y calidad en las recomendaciones, con esta se pretende que en la entidad se desarrolle un plan de capacitación, en donde se dé a conocer a la junta directiva las cualidades el auditor interno, para ampliar su rango de trabajo y que pueda servir de apoyo para la organización.

Siguiendo con el manual, es importante resaltar el desarrollo profesional, el cual manifiesta que debe ser continuo para que los auditores fortalezcan sus conocimientos y se garantice una mejora continua en todos los procesos de la organización, en la interpretación de la misma el

manual señala que los programas de capacitación para el aseguramiento de la información son vitales para el cumplimiento de los objetivos planteados, además que pueden llegar a mejorar la eficiencia del programa de auditoría.

En la empresa los auditores cuentan con un plan de capacitación de 40 horas como se mencionó anteriormente, al analizar el manual destaca que si se logra que los auditores se les programe un plan de capacitación suficiente, el logro de los objetivos será más eficiente. Para la organización en este momento cuenta con un cronograma de capacitación establecido, si bien se pudo evidenciar que estas son suficientes para el trabajo que se ha planificado, lo que se requiere es que el área de control interno pueda adelantar las fallas y cumplir con su labor de asesoramiento a la junta directiva.

En cuanto a la gestión de riesgos, el manual indica que ha estos se les debe evaluar e identificar cómo estos aportan a la mejora continua, es decir según la interpretación dada señala en una de sus directrices, que los riesgos deben ser evaluados de forma objetiva y lo más importante identificados. Es decir si la entidad XY cuenta con un departamento de riesgos para el análisis de los mismos, pero el caso de fraude como mejora la misma debería hacer partícipe al área de auditoría interna en los que son asociados al fraude, el conocimiento de los mismo permitirá que los auditores desarrollen su tarea de forma objetiva y con técnicas más eficientes, en la organización, en el plan de auditoría y antes de la elaboración del trabajo por parte del auditor, este estudia los mismos para verificar su trabajo, pero lo que se propone es que al área se le involucre en cómo fue su elaboración y como llegaron a la conclusión de que tanto puede afectar o no a la organización, si se conoce la fuente la generación de estrategias y de planes de mejora para la misma serán centrados hacia el objetivo de toda la organización, superando los del área.

En la elaboración de hallazgos la entidad como política tiene establecido que en las áreas de tecnología generen acciones inmediatas, pensado en calidad de la información y en el servicios que se le está prestando a los clientes. En este caso el auditor debe evaluar el tiempo, la solución y la respuesta que se brindó sí fue eficaz y eficiente para el usuario. Para este punto como mejora a la misma se propone que el área de control interno desarrolle una matriz donde se evidencian los hallazgos presentados más comunes, y cómo fue su solución con el fin de llevar un control preventivo hacia el área a la cual se le está aplicando la auditoría, a pensar de que los procesos de fraude son llevados por una empresa externa, la idea es que el departamento realice controles preventivos, que permitan anticiparse a los errores más frecuentes y que se han identificado con anterioridad.

Para la elaboración del plan de auditoría el cual se realiza anualmente, contemplando los niveles de exposición al riesgo, entregados por las áreas encargadas de los mismos y siguiendo las sugerencias del comité. Se plantea que en la entidad XY, en el área de control interno se le tenga en cuenta en los proyectos del departamento de desarrollo y tecnología, con el fin de que se conozca a fondo cómo fue su elaboración, y la implementación del mismo. Con esto el auditor que asista a las diferentes capacitaciones y secciones que se den en ese proceso contará con la debida capacitación y conocimiento para proponer cuál sería la forma y la técnicas que se puedan aplicar, con esto se espera que la labor de revisión y control supere las expectativas,

porque lo que se busca es que el auditor conozca el proceso de fondo, para anticiparse y generar alertas que ayude a la organización.

En una de las políticas mencionadas para la entidad XY, se definió que bajo ninguna circunstancia, los auditores desarrollen labores operativas o administrativas que no sean propias de su labor. Aclarando el punto anterior en donde se propone que los auditores tengan acceso a los proyectos que involucren al área de tecnología, que es por donde se canalizan los fraudes electrónicos, no se propone que estos tengan que aportar o dar recomendaciones, lo que se espera es que ellos efectúen una labor de aprendizaje en cuanto al desarrollo del proceso que se esté haciendo, con el fin de que en la elaboración del plan de trabajo se incluyan los puntos que ellos consideran son susceptibles a ser evaluados.

Para la política de responsabilidad de presupuesto, la cual es encargada por el administrador del proceso, se busca mostrar un paralelo entre las pérdidas que la entidad está teniendo por fraudes electrónicos y la inversión en recursos de personal, es decir que en la entidad XY, se realice un plan piloto, en donde se analicen cuantas personas se necesitan de acuerdo a la elaboración de los proyectos y mejoras de los mismos, esta información deberá ser entregada por el área de tecnología y por el área de riesgos, para que se pueda establecer cuáles son los de mayor impacto. Todo esto con el fin de demostrar que la labor de los auditores se podría desarrollar de forma eficiente, pues contaría con conocimientos desde el inicio del proceso y en su labor de revisión, llegarían a establecer cuáles podrían ser estos controles preventivos que las primeras líneas de defensa ejercerán.

En este momento la entidad XY se está viendo afectada por el aumento de pérdidas en fraudes, y en un porcentaje alto estos son electrónicos. En el análisis de la políticas se pudieron establecer que es posible la realización de un plan de mejora que involucre al área de control interno, si bien ya se revisaron cuáles pueden ser las posibles causas y las acciones de mejora que se pueden implementar, se hace necesario que la entidad realice un estudio de costos y recursos para que la viabilidad sea efectiva, lo que se quiere es que la organización identifique que desde el área de control interno se puede llegar a establecer un control preventivo, que sirva de apoyo para la toma de decisiones y los riesgos que la entidad evalúa, pensado no solo en la seguridad de la misma si no en la de los usuarios que si bien al finalizar el proceso recuperan sus pérdidas, la reputación o el buen nombre de la misma queda en dudas, pues no basta con demostrar que se están haciendo los esfuerzos y los controles que las entidades de vigilancia exigen, es necesario que se tomen medidas correctivas, y las anteriores propuestas es una prueba que la organización necesita conocer e implementar.

Para finalizar es importante mencionar que las acciones correctivas que se tomen, para los delitos de ciberseguridad deben ser continuas, esta no es una labor que se puede frenar, al contrario los delincuentes estudian nuevas posibilidades, y es lo mismo que las entidades deben hacer, en primera instancia tratar de combatir todos los frentes internos, y utilizar las ayudas tecnologías que se requieran, con el fin de mitigar los riesgos, reducir pérdidas y fidelizar a sus clientes.

CONCLUSIONES

Al finalizar el ensayo se puede concluir que después del análisis de diferentes casos, en donde los usuarios se estaban viendo afectados por fraudes electrónicos, la Corte suprema y la Superintendencia Financiera de Colombia han ido creando lineamientos para las entidades y así proteger los derechos de los clientes, en la investigación se muestran como los entes regulatorios después de las denuncias expuestas, impartieron instrucciones claras para estas entidades y algunas recomendaciones para generar buenas prácticas, es de aclarar que hoy en día, estas deben asumir las pérdidas por los fraudes de sus plataformas y devolver el dinero a sus clientes.

Con el avance tecnológico que está teniendo el mundo, las entidades financieras buscan herramientas que permitan facilitar el tiempo de las personas, estas deben ser probadas para mitigar los riesgos de seguridad y así no exponer la información de sus clientes, según anexos a las circulares vigentes de la Superfinanciera, las entidades deben evidenciar y establecer políticas que garanticen la seguridad de sus plataformas electrónicos.

En el análisis de ensayo. se explican las políticas y procedimientos de la entidad financiera XY, nombre que se utiliza para fines del presente trabajo, con el fin de brindar estrategias que mitiguen la pérdidas por fraude, que hasta finales de septiembre siguen aumentando con respecto al año anterior, en el mismo se recomienda que la entidad se apoye en el departamento de control interno, para que genere un control preventivo, vinculado al área en los diferentes desarrollos y mejoras tecnológicos que la entidad pretenda utilizar, la idea es que el auditor conozca el proceso de raíz, sin que haya lugar a labores operativas, si no que generen alertas en el momento de realizar la auditoría.

REFERENCIAS BIBLIOGRAFICAS

Asobancaria. (2019, 10 10). *Desafíos del riesgo cibernético*. asobancaria. Retrieved 11 3, 2020, from https://www.asobancaria.com/wp-content/uploads/20191010-asobancaria-OEA_min.pdf

Asobancaria. (2020, 08 1). *INFORME TARJETAS CRÉDITO*. Asobancaria. Retrieved 11 15, 2020, from https://www.asobancaria.com/informe-tarjetas-credito/

CISCO. (n.d.). *¿Qué es la ciberseguridad?* CISCO. Retrieved 11 8, 2020, from https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

EL TIEMPO. (2020, 09 28). Las denuncias por engaño bancario subieron 59 %. *Las denuncias por engaño bancario subieron 59 %.*, 1.

The Institute of Internal Auditors. (2017). *NORMAS INTERNACIONALES PARA LA AUDITORIA INTERNA*. https://www.iiacolombia.com/resource/Normas.pdf

Revista Portafolio. (2020, 07 17). Delitos cibernéticos crecieron 59 % en el primer semestre. Retrieved 11 13, 2020, from https://www.portafolio.co/economia/delitos-ciberneticos-crecieron-59-en-el-primer-semestre-542828

SFC. (n.d.). *Información financiera con fines de supervisión Bancos - NIIF*. superfinanciera. Retrieved 11 15, 2020, from https://www.superfinanciera.gov.co/inicio/informes-y-cifras/cifras/establecimientos-de-credito/informacion-por-sector/bancos/informacion-financiera-con-fines-de-supervision-bancos-niif-10084375

Superintendencia Financiera de Colombia SFC. (2020, 11 04). *Normativa General*. superfinanciera. Retrieved 11 05, 2020, from https://www.superfinanciera.gov.co/jsp/19167

Ustáriz, L. H. (2019). *Responsabilidad bancaria por fraude electrónico* (2nd ed.). Grupo editorial Ibañez.