RECOMENDACIONES PARA LA GESTIÓN DE LOS INCIDENTES DE SEGURIDAD ORIGINADOS EN EL ACCESO ABUSIVO A SISTEMAS DE INFORMACIÓN Y SUS REPERCUSIONES JURÍDICAS.

RENE ALEJANDRO TADINA GONZÁLEZ

LAURA HELENA VALDERRAMA LÓPEZ

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2017

RECOMENDACIONES PARA LA GESTIÓN DE LOS INCIDENTES DE SEGURIDAD ORIGINADOS EN EL ACCESO ABUSIVO A SISTEMAS DE INFORMACIÓN Y SUS REPERCUSIONES JURÍDICAS.

RENE ALEJANDRO TADINA GONZÁLEZ

LAURA HELENA VALDERRAMA LÓPEZ

Trabajo de grado para optar al título de Master en tecnologías de información y comunicación

Asesor

Arean Hernando Velasco Melo

Magíster en Informática y Derecho

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

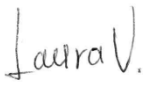
MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2017

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) _____  _____  _____

Medellín, Julio 27 de 2017

AGRADECIMIENTOS

A nuestras familias, quienes han sido parte fundamental durante este proceso de formación académica ya que con su comprensión y sacrificio se convirtieron en el motor que siempre nos impulsó a terminar con éxito este capítulo de nuestras vidas.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: el que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. (Congreso de la República de Colombia, 2009a)

CONSUMIDOR FINANCIERO: es todo cliente, usuario o cliente potencial de los productos o servicios ofrecidos por las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera, así como todo aquel que determine la Ley o el Gobierno Nacional. (Congreso de la República de Colombia, 2009b)

ENTIDAD FINACIERA: entidad que presta servicios financieros a sus clientes, es decir, una compañía que ofrece a sus clientes (familias, empresas, Estado) servicios relacionados con el dinero que posee o necesita. (MP, 2012)

MAN IN THE BROWSER: es un troyano que tras infectar una maquina es capaz de modificar páginas webs, contenidos o transacciones, de una manera invisible tanto para el usuario como para el servidor web.(Alegre & García, 2011)

MAN IN THE MIDDLE (HOMBRE EN EL MEDIO): esta amenaza consiste en interceptar y modificar la comunicación entre dos equipos. (Alegre & García, 2011)

PHARMING: es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System). (Alegre & García, 2011)

PHISHING O SUPLANTACIÓN DE IDENTIDAD: se caracteriza por intentar adquirir información confidencial y hacerse pasar por una persona o empresa. (Alegre & García, 2011)

PRINCIPIO DE RESPONSABILIDAD: por el que se entiende que la realización de operaciones a través de Internet es posible únicamente porque las entidades han implementado este sistema (con los mecanismos de seguridad y autenticación que han considerado convenientes), y lo han divulgado, adquiriendo por ello una responsabilidad respecto del buen funcionamiento y la seguridad del mismo. (Sachis, 2011)

RANSOMWARE: es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.(Alegre & García, 2011)

TROJANO: se denomina caballo de Troya a un software malicioso que se presenta al usuario como un programa aparentemente legitimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. (Alegre & García, 2011)

RESUMEN

En la actualidad las tecnologías de la información y las comunicaciones han permitido al internauta y usuarios en general el acceso rápido a la información sin importar el lugar donde se encuentre; tal alcance obliga al dueño o administrador de los sistemas de información a generar estrategias que aseguren y permitan el acceso a los activos únicamente al personal autorizado.

En el evento que alguien acceda de manera abusiva o no autorizada a la información contenida en el sistema, tal acción podrá tener trascendencia jurídica penal, civil, laboral y disciplinaria que buscará el restablecimiento del derecho para la víctima y la judicialización para la persona o personas que accedieron sin la debida autorización, sin perjuicio de otras repercusiones jurídicas.

Es necesario abordar el acceso no autorizado a sistemas de información desde dos enfoques:

- Jurídico
- Tecnológico

Los cuales se consideran fundamentales para el análisis, implementación, y control de los procesos de aseguramiento de la información.

Como estrategias para el tratamiento del riesgo derivado del acceso no autorizado, en este trabajo de grado se elaboraran una serie de recomendaciones que servirán de apoyo a la comunidad financiera mitigando el impacto que se representa en pérdidas económicas para quienes se constituyen víctimas, disminuyendo la materialización de hechos que afecten la reputación de la entidad financiera responsable de la administración de la información que es provista por el cliente.

PALABRAS CLAVE: Control de acceso; legislación; seguridad; información; gestión.

ABSTRACT

Currently, information technology and communications have permitted Internet users and general users' quick access to information no matter where they are; such scope requires the owner or manager of information systems to generate strategies that ensure and allow access to assets to authorized personnel only.

In the event that someone accesses misused or unauthorized to information contained in the information system, such action may have criminal legal significance that seek the restoration of the right for the victim and the prosecution for the person who accessed without the authorization, without prejudice to other legal implications.

It is necessary to address unauthorized access to information systems access from two approaches:

- Legal
- Technology

Which are considered essential for analysis, implementation, control and assurance processes information.

As strategies for the treatment of risk arising from unauthorized access, this paper grade a series of recommendations that will support financial institutions and financial consumers mitigating the impact represented in economic losses be developed for those victims are, decreasing the materialization of events that affect the reputation of the administration responsible for the information that is provided by the client financial institution.

KEY WORDS: Access control; legislation; security; information; management.

1 INTRODUCCIÓN

En la industria financiera, entre otros, existen dos protagonistas a los que de aquí en adelante se hará referencia, estos son: entidad financiera y consumidor financiero.

Se infiere que la entidad financiera podría autosostenerse por si sola al ser experta en lo que se refiere a la actividad comercial y financiera, sin embargo esta no subsistiría sin la intervención del consumidor, quién a su vez es casi que condicionado a acceder por lo menos a uno de los productos ofrecidos en el mercado financiero, circunstancia necesaria para la mayoría de los ciudadanos, por ejemplo, el pago de salario a través del producto dé cuenta de ahorros o el préstamo de dinero a través de desembolsos crediticios.

Si se analiza el rol de cada protagonista, podemos ejemplificarlo a manera de líneas de defensa; es el caso por ejemplo de los cuentahabientes a quienes se les expide un plástico para acceder al servicio de retiro de efectivo a través del canal electrónico cajero automático y/o físico oficina, estos se obligan a conservarlo con las debidas seguridades y manteniendo absoluta reserva en su número de clave personal, lo que se denomina primera línea de defensa. Esta primera línea de defensa en cabeza de millones de ahorradores y/o consumidores financieros lamentablemente puede ser vulnerada por el actuar delincuencial y la falta de deber de cuidado en el manejo de la información.

La segunda línea de defensa aparece en escena con el propósito de proteger precisamente al consumidor financiero, en el entendido que son las entidades financieras quienes cuentan con la experticia, elementos técnicos y humanos para ejercer la actividad financiera.

Existe una tercera línea de defensa a través de la cual el consumidor financiero cuenta con la acción respectiva ante la justicia ordinaria y/o ante la justicia especializada, en este caso la superintendencia financiera de Colombia, quien basada en el análisis de los hechos y la exigencia de la debida aplicación de la normatividad vigente, debe objetivamente determinar a cuál de los protagonistas le asiste la responsabilidad frente a los hechos objeto de litigio.

Con base a lo anteriormente expuesto, se observa la necesidad de ilustrar mediante el presente documento de recomendaciones, el deber de cuidado acerca del manejo de la información financiera por parte de los protagonistas, mitigando así la materialización del riesgo a través del delito de acceso abusivo a sistemas informáticos y presentando posibles soluciones antes, durante y después de la relación comercial y financiera, focalizados en tres componentes, jurídico, tecnológico y gerencial.

Es entonces necesario que cada protagonista conozca:

- Los riesgos que se derivan de esta relación y la responsabilidad que corresponde a cada uno.
- Los mecanismos de defensa a los que cada uno tiene derecho en caso de que surjan hechos sobrevinientes a la relación comercial que afecten el patrimonio económico y/o la información y los datos.
- Las herramientas y controles que cada uno debe adoptar en lo que se refiere a la prevención del acceso abusivo a sistemas informáticos.
- Las instancias administrativas, legales y/o judiciales a las que se puede acudir en caso de la materialización de este delito.

2 PLANTEAMIENTO DEL PROBLEMA

2.1 Problema

Dada la realidad que enfrenta nuestro país con respecto a la cibercriminalidad y que las pérdidas más representativas se reflejan en la industria del sector financiero, es necesario dar a conocer a través de recomendaciones la adecuada gestión de incidentes de seguridad derivados del acceso abusivo y sus repercusiones jurídicas.

Cada vez que la industria financiera (consumidor o entidad) es víctima de acceso abusivo a un sistema informático afectando las propiedades de un sistema seguro como lo son la confidencialidad, integridad y disponibilidad de los datos, se evidencian falencias en:

- Conocimiento, cultura de protección y deber de cuidado de la información por parte del consumidor financiero
- Carencia de políticas adecuadas que aseguren el bien jurídico tutelado de la información y los datos por parte de las entidades financieras que administran la información
- Falta de claridad por parte de la entidad financiera en el manejo de los incidentes de seguridad, derivados del acceso abusivo una vez se han materializado.
- Falta de inversión económica por parte de las entidades financieras que permita la adquisición de herramientas eficaces para la prevención del acceso abusivo a sistemas informáticos en los cuales se almacena y administra información y datos personales y financieros del consumidor.
- Falta de transparencia por parte de la entidad financiera con el consumidor al momento de celebrar el contrato del producto adquirido.

La entidad gubernamental encargada de supervisar a las entidades financieras y en general el movimiento bursátil y de valores de Colombia es la SFC Superintendencia Financiera de Colombia, sin embargo las disposiciones emitidas en la circular externa 042 (Superintendecia Financiera de Colombia, 2012) que obligan a las entidades financieras en lo que se refiere a requerimientos mínimos de seguridad y calidad de las operaciones a través de los diferentes canales, son muy generales, pues estos mecanismos que pretenden proteger la información y los datos personales en algunos casos son desconocidos por el consumidor financiero y en el momento de establecer la relación contractual y comercial entre las partes, la entidad financiera-consumidor no se brinda a este último con claridad la totalidad de la información que le permita conocer sus derechos y obligaciones , además de las repercusiones jurídicas que implican el incumplimiento de las disposiciones para cualquiera de las partes en especial la entidad financiera que es la experta en operación bancaria.

Las casusa, Figura 1, y consecuencias, Figura 2, más comunes del problema de cibercriminalidad en Colombia, Figura 1, se detallan en los resultados mostrados por la encuesta KPMG (KPMG Advisory Services Ltda., 2013).

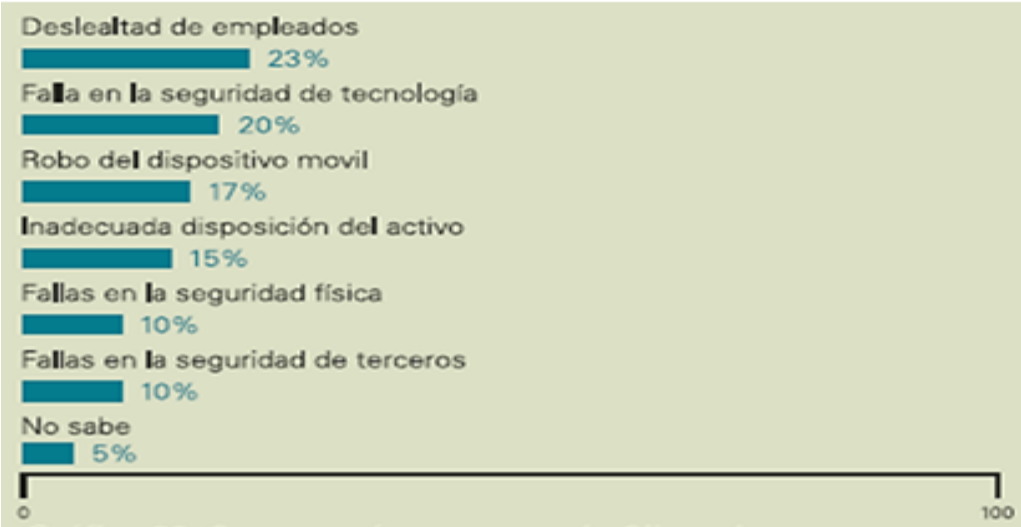


Figura 1. Causas de la cibercriminalidad
Fuente: Encuesta de Fraude en Colombia 2013, KPMG Advisory Services Ltda. (2013).

Figura 2. Consecuencias de la cibercriminalidad
Fuente: Encuesta de Fraude en Colombia 2013, KPMG Advisory Services Ltda. (2013).

Actualmente, el colCERT es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa, el cual presta su apoyo y colaboración a las instancias nacionales tales como el CCP y el CCOC. Este organismo elaboro un estudio de incidentes digitales de seguridad por el cual se obtuvieron las siguientes estadísticas, figura 3, para el año 2015.

Figura 3. Incidentes digitales en Colombia
Fuente: Consejo nacional de política económica y social- política nacional de seguridad digital, (Álvarez, 2016)

Realizando entrevistas y trabajo de campo a la sala de análisis criminal SAC de la Fiscalía General de la Nación a través del cuerpo técnico de investigación judicial CTI, se encontraron las estadísticas actualizadas, Figura 4, de algunos delitos que afectan el bien jurídico de la información y los datos en área metropolitana de valle de aburra.

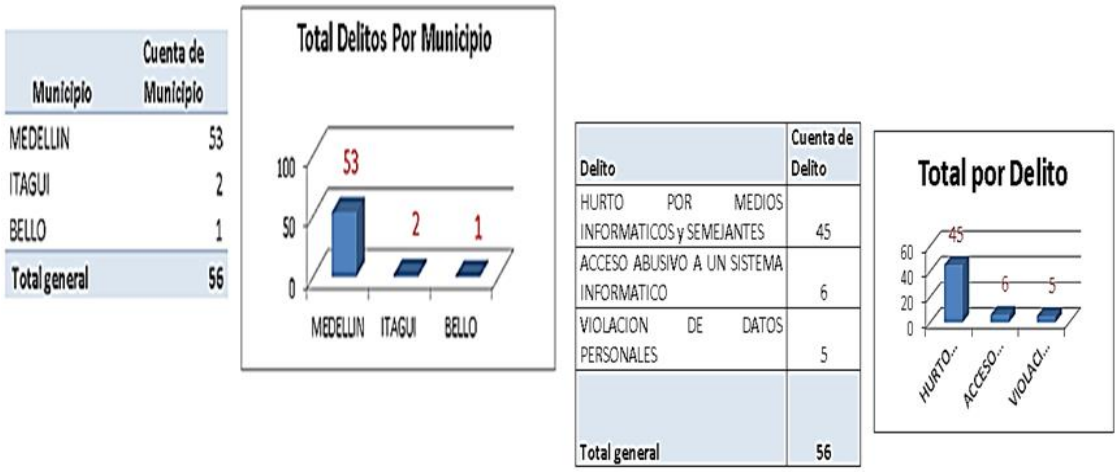


Figura 4. Delitos Informáticos Medellín y área metropolitana
Fuente: Informe Dinámica Delictiva Delitos Informáticos (Sección análisis criminal direccion nacional de seccionales y seguridad, 2015)

2.2 Justificación

La motivación de llevar a cabo este proyecto se basa fundamentalmente en las pérdidas económicas de la industria financiera derivadas del acceso abusivo a sistemas informáticos y el desconocimiento general de cómo prevenirlo; también en caso de materializado el delito, cómo lograr el restablecimiento del derecho que en ocasiones se dificulta por la falta de claridad de la información al consumidor financiero por parte de la entidad, inclusive desde el inicio de la relación comercial.

Es necesario realizar un tratamiento acorde a las causas identificadas que minimicen sus efectos atacando directamente a las falencias enmarcadas en los siguientes puntos:

- La fuga de información y el acceso no autorizado que provocan una violación a la privacidad además de pérdida o modificación de la información.
- El incorrecto funcionamiento de los sistemas de información que ocasiona afectación del servicio y falta de disponibilidad de la información.
- Pérdida de confidencialidad de la información que genera un riesgo reputacional para las entidades y además puede conllevar a pérdidas económicas.

Aunque las entidades financieras están obligadas a brindar a sus clientes la asesoría, herramientas necesarias para la protección de la información y la prevención del acceso no autorizado, los medios y canales de comunicación utilizados con los cliente y/o usuarios en ocasiones no son eficaces puesto que se hacen posterior al inicio de la relación comercial y a través de medios que quizá el consumidor no accede o no conoce por diferentes circunstancias.

Teniendo en cuenta que las tecnologías la información y las comunicaciones si bien es cierto han facilitado a la comunidad financiera el acceso a productos y servicios se considera que las entidades financieras deben brindar la evidencia electrónica, física y digital respecto de los hechos que caracterizaron el acceso abusivo, con el fin de que el ciudadano tenga derecho a verificar si el acceso abusivo ocurrió como consecuencia de una mala práctica propia o si fue resultado del hecho de un tercero; caso en el cual, el dinero al estar en poder del banco, quien debería asumir la perdida es el banco y no el usuario del sistema.

Con este proyecto se pretende sensibilizar a la comunidad acerca del uso adecuado que debe darse a la información y datos contenidos en las entidades Financieras, a través de un conjunto de recomendaciones se busca poder minimizar los incidentes que se deriven del acceso abusivo a sistemas informáticos.

Se considera que si dichas recomendaciones son adoptadas y puestas en práctica, el impacto para la sociedad será positivo; a continuación se detallan dos aspectos que se consideran relevante para el trabajo en mención: Primero, se disminuyen las pérdidas económicas que se producen por la materialización del delito de acceso abusivo a sistemas informáticos, además de los costos en que se incurre al someterse a un proceso legal para la recuperación del dinero y/o información hurtada. Segundo, se tendría mayor confianza por parte de los clientes para hacer uso de las banca electrónica, consiguiendo con este punto la disminución de delitos como el fleteo que permanentemente cobra la vida de más personas.

3 OBJETIVOS

3.1 Objetivo General.

Construir un documento de conceptos y recomendaciones dirigido a la comunidad financiera, que permita el correcto manejo de los incidentes de seguridad originados en la gestión de accesos a sistemas de información, así como también las repercusiones jurídicas de dichos incidentes.

3.2 Objetivos Específicos

- Caracterizar los incidentes de seguridad de la información derivados del acceso abusivo a entidades financieras
- Describir las repercusiones jurídicas asociadas a un incidente de seguridad por acceso abusivo a un sistema de información.
- Informar a la comunidad acerca de los aspectos legales vinculados a un incidente de seguridad de la información en el sector financiero.

- Elaborar un instructivo con recomendaciones a partir de los enfoques tecnológico y jurídico para la mitigación del riesgo de acceso abusivo a sistemas de información en la industria financiera.

4 MARCO REFERENCIAL

4.1 Marco contextual

Las entidades financieras como parte de la industria ejercen la labor de un comerciante experto que se lucra con su actividad a diferencia de los clientes y/o usuarios que aunque hacen parte de esta industria no necesariamente son expertos en dicha actividad, ya que su interés podrá ser particular de acuerdo a la necesidad.

Los comportamientos que le son exigibles a las entidades financieras en las transacciones ´´on-line'' surgen a partir de unas premisas, que a su vez dan a luz algunos principios, lo anterior de acuerdo a lo establecido por la doctrina (Sachis, 2011) y jurisprudencia internacional (Jurisprudencia internacional, 2009)

Premisa 1: Son las entidades del sector financiero las que han puesto en funcionamiento el canal transaccional para sus clientes, cuyo uso fraudulento puede devenir en graves perjuicios para los mismos

Premisa 2: El uso fraudulento puede venir producido no solo por la negligencia de los clientes, sino por un desconocimiento más que comprensible de los riesgos asumidos o por la vulnerabilidad de los sistemas de autenticación utilizados.

Premisa 3: Los sistemas de autenticación son elegidos por las entidades financieras, existiendo casos en los que otros sistemas pueden proporcionar mayor seguridad para los clientes al momento de autenticarse en el sistema.

Infiriendo de manera razonable la aplicación inmediata del decreto 1074 de 2015 sección 6 (Congreso de la República de Colombia, 2015) en lo que respecta al principio de responsabilidad demostrada y que aunque se pudiera pensar que las entidades financieras vigiladas por la Superintendencia financiera de Colombia cumplen con lo descrito en las circulares externas 052 de 2007 y 042 de 2012, existe un vacío en cuanto a la responsabilidad demostrada, ya que aunque la industria financiera en cabeza de las entidades establecen políticas, procedimientos y continuamente implementan herramientas y mejoras tecnológicas en lo concerniente a la seguridad y la calidad de los diferentes canales a través de los cuales se ofrecen productos y servicios, no se cumple a cabalidad con lo exigido por la ley decreto 1377 de 2013 artículo 27, un ejemplo de lo mencionado es la desproporción de las cargas de responsabilidad que la entidad financiera le descarga en el cliente, este último aceptándolo de manera casi inconsciente pensando más en la necesidad de acceder al producto financiero y no en las

calidades adquiridas de acuerdo al contrato que está firmando al momento de la adquisición del producto.

4.2 Marco conceptual

Las medidas de seguridad que deben ser adoptadas e implementadas para la protección de la información y con estas mitigar la materialización del riesgo a través del acceso abusivo se conocen como buenas prácticas de seguridad.

El desarrollo de la tecnología ha contribuido al actuar delincuencial permitiendo entre las diferentes modalidades el acceso de forma abusivo a la información y los datos, sin embargo este desarrollo tecnológico es una pieza fundamental en la creación de herramientas técnicas que ayuden a la prevención, detección y judicialización de estos delincuentes; constituyéndose así el desarrollo de la misma en un aliado estratégico para las entidades financieras, siempre y cuando se realice inversión y selección las herramientas adecuadas.

En lo concerniente al desarrollo tecnológico de los canales transaccionales, el sector financiero colombiano ha tratado de estar a la vanguardia y son de gran importancia los avances en términos de migración hacia sistemas inteligentes de seguridad, tales como: la autenticación de la identidad de los clientes, configuración de perfiles transaccionales, el monitoreo y respuesta de información en línea de operaciones realizadas; no obstante además de estos desarrollos es necesario que los clientes y usuarios del sistema financiero adopten las medidas de seguridad necesarias en los equipos y dispositivos desde los cuales realizan las transacciones, así como el deber de cuidado que deben tener de su información financiera y datos personales.

Se considera evidencia digital al ´´tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales´´ (Diana, Prieto, & Peña, 1999). Es importante tener en cuenta que la evidencia digital es parte fundamental en el desarrollo de cualquier proceso en el que se considere que se cometió delito de acceso abusivo así como cualquiera de sus respectivos elementos, y procedimientos que permitan a los responsables establecer directrices claras sobre la administración de esta clase de evidencias, serán tenidos en cuenta para este.

Internet y los medios electrónicos a diario se utilizan para realizar negocios a nivel nacional e internacional dado que son los instrumentos más rápidos para realizar transacciones en cuestiones de segundos, estas transacciones generan efectos y consecuencias jurídicas (Cano Martínez, 2010); por tal razón al hablar de este tipo de consecuencias, los medios electrónicos y las transacciones como tal son susceptibles de ser valoradas como pruebas en un escenario jurídico y/o judicial derivadas de alguna irregularidad o actividad fraudulenta, escenario que es común en la actividad financiera.

En lo que concierne a la correcta valoración de la evidencia digital a nivel nacional e internacional, que en ocasiones puede verse afectada por una valoración deficiente por parte del juez y para la cual se requiere que sea muy clara y detallada, inclusive más que cualquier otro medio probatorio, han surgido países en la comunidad europea pioneros en la materia como Alemania, Italia y España en donde se otorgó a la firma electrónica el mismo valor jurídico de la manuscrita, en Colombia desde el año 1999 reconoció ese valor ya mencionado, esto con la ley 527 de 1999.

El ciclo de vida para la administración de la evidencia digital, Figura 5, consta de seis pasos (Cano, 2015):

1. Diseño de la evidencia
2. Producción de la evidencia
3. Recolección de la evidencia
4. Análisis de la evidencia
5. Reporte y presentación
6. Determinación de la relevancia de la evidencia

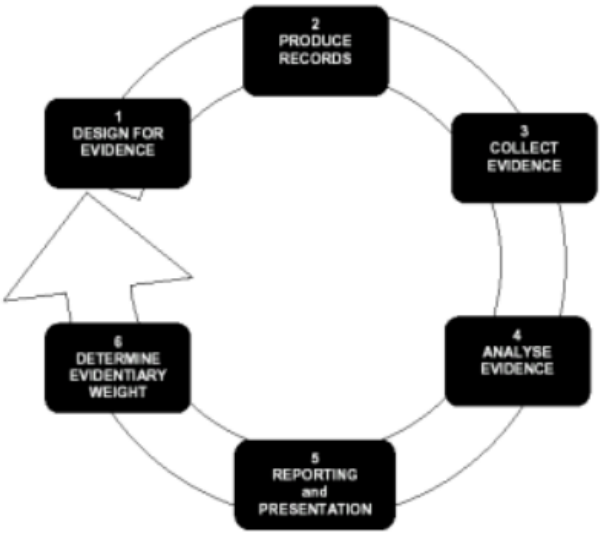


Figura 5. Ciclo de vida para la administración de la evidencia
Fuente: Guidelines for the Management of IT Evidence (APEC Telecommunications and Information Working Group, 2004)

Se puede decir que el manejo que se le da a la evidencia digital va ligado o está directamente relacionado con el análisis forense, el cual se le aplica directamente a la evidencia digital y este consta de cinco pasos principalmente (Lopez, 2007):

1. Adquisición de evidencia: En esta fase se realiza copia de seguridad a aquella información que se considera relevante o involucrada en un incidente de seguridad particular

2. Preservación: En esta fase se garantiza que la evidencia recolectada no sea alterada o eliminada y que se conserve como fue recolectada inicialmente

3. Análisis: En esta fase se hace un análisis de la información recolectada mediante software especializado en el tema que permitirá detectar algún evento o suceso que implique o de indicio de delito.

4. Documentación: en esta fase se recopilan y documentan los resultados obtenidos del análisis.

5. Presentación: En esta fase se entrega un informe ejecutivo que de una forma comprensible muestre los resultados obtenidos del proceso anteriormente mencionado.

El nivel de madurez con el que se maneja la seguridad de la información estará relacionado directamente con:

- Establecer un orden claro, discreto y absoluto, definiendo niveles y etapas de madurez.

- Establecer de manera explícita la evolución de las organizaciones en dicho aspecto.

- Lo anterior permitirá a la entidad u organización establecer unos objetivos de seguridad y los alcances requeridos, así como oportunidades de mejora y alineación con estrategias organizacionales.

Para establecer el nivel de madures con que cuentan las organizaciones, existen diversos modelos internacionales, los cuales pueden ser adoptados por estas para alcanzar un nivel deseado, estos son (Cissp, 2007)

- NIST-CSEAT

- CITI-ISEM

- COBIT Maturity Model

- ISM3

- SSE-CMM

Al igual es importante mencionar estándares internacionales como lo es la ISO 27002, en donde en uno de sus dominios, como lo es el cumplimiento, enmarca elementos fundamentales para la seguridad de la información: cumplimiento de los

requisitos legales exigidos para las organizaciones en general, en donde se debe evitar el incumplimiento de cualquier ley de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad. El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad estatutarios, reglamentarios y contractuales (International Organization for Standardization/ International Electrotechnical Commission, 2013a)(International Organization for Standardization/ International Electrotechnical Commission, 2013a).

4.3 Marco legal

4.3.1 Leyes

Convenio de cibercriminalidad Budapest 2001

Contenido: El presente convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el convenio, y la asunción de dichos poderes suficientes para luchar eficazmente contra dichos delitos.

Ley 527 de 1999 (Congreso de Colombia, 1999):

Contenido: Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012).

Ley 1266 de 2008 (Congreso de la República de Colombia, 2008)

Contenido: Contempla las disposiciones generales en relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009 (Congreso de la República de Colombia, 2009a)

Contenido: Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC”.

Ley 1581 de 2012 (Congreso de la República de Colombia, 2012b)

Contenido: Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.

Ley 1712 de 2014 (Congreso de la República de Colombia, 2009)

Contenido: Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.

Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 –Alemania

Contenido: Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita.

Ley de reforma del Código Penal del 22 de diciembre de 1987- Austria

Contenido: Estafa informática (art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993- Chile

Contenido: El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) de 1994- Estados Unidos.

Contenido: Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

Electronic Signatures in Global and National Commerce (Act. 2000)

Contenido: Establece Por regla general de validez de los documentos electrónicos y firmas para las transacciones en o que afecten el comercio interestatal o extranjero. La Ley de E -Sign permite el uso de registros electrónicos para satisfacer cualquier ley , reglamento o norma de ley que exige que tales la información se facilitará por escrito , si el consumidor tiene afirmativamente su consentimiento para dicho uso y no haya retirado tal consentimiento .

4.3.2 Artículos

Artículo 15 C.N (Constituyente, 1991)

Contenido: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Artículo 269a Ley 1273 de 2009

Contenido: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

4.3.3 Decretos

Decreto 4327 de 2005:

Contenido: Por el cual se fusiona la Superintendencia Bancaria de Colombia en la Superintendencia de Valores y se modifica su estructura.

Decreto 1747 de 2000: (Soediono, 2000)

Contenido: Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales

Decreto 1727 de 2009

Contenido: Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

Decreto 1074 de 2015 (Sección 6)

Contenido: Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012

Sentencia T 729 de 2002:

Contenido: Trata temas jurídicos tan importantes como el contenido y el alcance del derecho constitucional del Habeas Data o la autodeterminación informativa

Sentencia SC18614 del 2016 Fraude Electrónico

Contenido: Trata temas como la teoría del riesgo creado, responsabilidad objetiva y la diligencia exigible a las entidades financieras.

Decreto 886 de 2014

Contenido: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

4.4 Estado del arte.

Actualmente en Colombia se cuenta con la ley 1273 de enero 5 de 2009 a través de la cual se protege el bien jurídico de la información, los datos y de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, tipificada en el artículo 269a de la presente ley.

Es necesario mencionar la ley 527 de 1999 que reconoce el equivalente funcional entre el documento electrónico y el documento físico, y reconoce el mensaje de datos como aspecto que tiene validez legal y eficacia probatoria.

Realizando una análisis en algunas de las entidades financieras en lo que respecta a los contratos de vinculación de clientes con productos como: cuentas corrientes, ahorros y demás, se determina que la carga de la responsabilidad del deber de cuidado y administración de la información está en cabeza del cliente y no de la entidad financiera experta en la operación bancaria, y si bien es cierto la entidad financiera vigilada por la SFC en cumplimiento de los requerimientos mínimos de

seguridad establece lineamientos y herramientas que garanticen la seguridad y la calidad en los diferentes canales a través de los cuales las entidades financieras ofrecen el acceso a sus productos y servicios, mencionados en los incisos 3.4.4, 3.4.5 y 3.4.6 de la circular 042 (Superintendecia Financiera de Colombia, 2012), no se le está informando al cliente a través del contrato de vinculación:

- Los riesgos a los que se puede ver expuesto al utilizar la red para comunicarse con su banco.
- Las medidas de seguridad que debería implementar en su máquina y en la red evitando así el acceso abusivo.
- El cuidado que debe tener acerca de la custodia de los dispositivos de autenticación (Token o kits biométricos).
- La responsabilidad que se adquiere al tener a su disposición usuarios y contraseñas, y la confidencialidad que se debe tener con estos.
- La capacitación que debe brindarse al cliente al momento de la vinculación o de la habilitación del portal electrónico para el uso de los productos y servicios, condiciones que debía ser obligatorias para la utilización de este.

Haciendo un análisis del incremento de los delitos informáticos en el sector financiero a finales del año 2015, Figura 6, y mediante entrevista a algunos clientes de diferentes entidades financieras que han sido víctimas de acceso abusivo a sistemas informáticos y que derivado de este se han generado pérdidas considerables, se puede decir que en una sola transferencia no consentida derivada de acceso abusivo se han generado pérdidas de hasta 50 millones de pesos por transacción y las respuestas por parte de la entidad financiera ante la reclamación de estos clientes, es la negación a la solicitud de devolución de dineros, descargando toda la responsabilidad del deber de cuidado sobre el cliente ya que la entidad financiera al evidenciar el más mínimo detalle que demuestre falencias o debilidades en la utilización del portal virtual bancario, salva su responsabilidad negando la petición del cliente con respecto al restablecimiento de los valores defraudados.

Figura 6. Fraude electrónico
Fuente: Fraude en transacciones ACH (Comité prevensión Fiscalia general de la Nación, 2016)

Es importante mencionar que algunas entidades financieras entregan documentación anexo al momento de habilitar el portal virtual y no al momento de la vinculación y dicha documentación no posee el carácter de obligatoriedad, si no que inclusive en algunas ocasiones el título de esas recomendaciones entregadas de forma física al cliente es simplemente ´´tenga en cuenta''. Además no se utilizan diversos canales de distribución para dar a conocer al cliente las medidas de seguridad que debe adoptar, debido a que los utilizados actualmente no garantizan que los clientes los lean, entiendan y apliquen.

A raíz de lo mencionado en lo que respecta a diferentes modalidades de delitos informáticos las legislaciones de varios países de Latinoamérica han efectuado cambios importantes en las codificaciones penales, en donde si bien no se contempla la figura “delito informático”, se han empezado a tipificar y contemplar el uso de mecanismos tecnológicos para cometer conductas antijurídicas clásicas y nuevas. Al respecto es importante citar el caso de Chile que fue uno de los primeros países en sancionar una Ley Contra los Delitos Informáticos denominada como 19223, publicada en el diario oficial el 7 de junio de 1993; resaltando además el caso de la República Argentina que tiene una Ley de Delitos Informáticos la cual es denominada con el número 26388.(Romo Santana, 2013)

Es importante entonces mencionar la sentencia de la audiencia provincial de Valladolid, Unión Europea, de 10 de marzo de 2010 en la que se establece que los relevante no el sistema utilizado, que siempre es mejorable, mientras resulte apto,

sino que el cliente comprenda los riesgos de aceptar el sistema de autenticación ofrecido por la entidad con la que opera y que conozca cuál es la mejor alternativa posible para poder prevenir el fraude.(Sachis, 2011)

Es relevante mencionar que las pruebas establecidas para los delitos por acceso abusivo a un sistema de informáticos son pruebas meramente electrónicas; en Colombia a pesar de que en la actualidad se cuenta con normatividades que regulan las transacciones y negocios mediante correos electrónicos, páginas web y otros campos de acción ofrecidos por la internet, existe una problemática sobre la valoración de las pruebas digitales aportadas en un proceso determinado, ya que estas pueden generar dudas en cuanto a la confidencialidad, integridad y autenticidad de la información presentada en formato de mensaje de datos u otro tipo de documento electrónico. El resultado de esto es que tales pruebas sean valoradas solo como indicios o por el concepto técnico de un perito; aunque ambos son idóneos para brindar certeza al juez acerca de los hechos, aminoran la fuerza probatoria de la evidencia digital impidiendo que entren a un proceso como una prueba en sí. (Cano Martínez, 2010)

De acuerdo a la ley colombiana en el artículo 164 del código general del proceso (Congreso de la República de Colombia, 2012), en lo que respecta a la valoración que debe realizar el juez, este debe dirimir cualquier controversia a partir de las pruebas que consten en el proceso y más adelante en el artículo 165 hace referencia puntualmente al dictamen pericial como medio de prueba.

Acerca de la valoración de las pruebas en Colombia, el artículo 176 del código general del proceso (Congreso de la República de Colombia, 2012) indica que las pruebas deben ser apreciadas en conjunto, lo que quiere decir que no podrá fallar por la simple valoración de una de ellas, si no por el convencimiento que sea el resultado de la pluralidad de las pruebas allegadas oportunamente al proceso.

De acuerdo a lo planteado en los párrafos anteriores concerniente a los medios de prueba y a la valoración que debe hacer el juez de estas, es importante mencionar que aunque existe una diferencia entre las pruebas procesales y las extraprocesales, dando quizá a esta ultima un menor valor ya que no se realiza delante del juez, prevalece la procedencia de la prueba de acuerdo al artículo 226 del código general del proceso, el cual hace referencia directamente a la prueba pericial resaltando que es procedente siempre y cuando la verificación de los hechos objeto del peritazgo aporten al proceso. De esta manera a la luz del artículo 165 del código general del proceso el cual hace referencia a los medios de prueba y que dentro de estos se incluye el dictamen pericial este inclusive puede practicarse como prueba extraprocesal de acuerdo al artículo 183 del código general del proceso, siendo así susceptible de ser valorada por el juez con el fin de encontrar la verdad conforme a los hechos acecidos.

5 METODOLOGÍA

La metodología utilizada para el desarrollo de este proyecto fue cualitativa a través del método descriptivo, pues se elaboró un estudio de casos acerca del acceso abusivo a sistemas de información a entidades financieras y consumidores financieros, además de las repercusiones jurídicas que de estos se derivan; identificando de esta forma el modo de operar de aquellas personas dedicadas a cometer el delito de acceso abusivo a sistemas informáticos y cuáles son las debilidades asociadas con este delito a través de las omisiones generalmente cometidas por los consumidores financieros y/o acciones erróneas que facilitan esta comisión delictiva; permitiendo de esta manera, generar una serie de recomendaciones objetivas a la industria financiera para la mitigación de este inminente riesgo de seguridad de la información, presentando no solamente el problema, sino la posible solución a partir de dichas recomendaciones a los protagonistas consumidor-entidad.

Dentro del desarrollo de esta investigación para el alcance de los objetivos propuestos se utilizaron instrumentos de investigación tales como: entrevista, observación, análisis documental y dinámica de grupos.

Las fases desarrolladas en la metodología a la luz de los objetivos específicos y que por ende generan los resultados esperados en el proyecto, son las siguientes

1. Fase I: Recolección de información.

Se recopilo información a partir del conocimiento adquirido de forma teórico practica mediante el contacto directo con las áreas de seguridad de algunas entidades financieras y la atención e investigación a consumidores financieros victimas de acceso abusivo a un sistema informático, para lo cual en particular se revisaron los casos denominados fraudes a través de medios informáticos durante los periodos 2015 y 2016 de una entidad financiera en particular, detectando las posibles causas, acciones u omisiones de la industria financiera, entidad financiera y consumidor financiero, que facilitaban este tipo de fraude. Además se recogió información proveniente de varias entidades financieras asociada con el delito de acceso abusivo a un sistema de información solicitando la misma a través de correo electrónico enviado el 23 de enero de 2016 directamente a las áreas de seguridad de los bancos que pertenecen al frente de seguridad bancario de la ciudad de Medellín y área metropolitana, entre ellos, Bancoomeva, Banco Caja Social, Banco Agrario, Cooperativa Financiera de Antioquia, Bancamia, Bancolombia, Citibank, Banco de Bogotá, AV villas, Incocredito, Banco de Occidente, entre otros.

Posterior a esta actividad se recolectaron y analizaron estadísticas relacionadas con la misma modalidad delictiva antes mencionada siendo estas suministradas por la sala de análisis criminal de la Fiscalía General de la Nación, trabajo que se llevó a cabo de forma presencial en las instalaciones del bunker de la fiscalía de la ciudad

de Medellín siendo atendidos directamente por la coordinación de la sala de análisis criminal lo anterior se realizó con el objetivo de identificar y caracterizar comportamientos específicos para el acceso abusivo en Colombia y la región de Antioquia.

Teniendo en cuenta que el problema planteado en este documento tiene que ver con un delito tipificado en la ley colombiana se hizo necesario escudriñar la jurisprudencia colombiana, las leyes, decretos, y sentencias para las cuales aplica el delito de acceso abusivo en Colombia, sin dejar a un lado el derecho comparado aplicado en otros países para este delito.

2. Fase II: Análisis y caracterización de los incidentes de seguridad de la información derivados del acceso abusivo a la industria financiera.

Dentro de los denominados fraudes informáticos coexisten varios delitos que afectan los bienes jurídicos de la información y los datos, además del patrimonio económico, sin embargo a partir del análisis realizado se consideró que el delito de acceso abusivo a un sistema informático puede propiciar otros incidentes de seguridad que se materializan a través de estos medios.

A partir del análisis de la información recolectada, se consideró indispensable enunciar los incidentes de seguridad que pueden derivarse del acceso abusivo, incidentes que constantemente se materializan afectando a la industria financiera por lo que es importante darlos a conocer.

Una parte de este proyecto se enfocó en la investigación cuantitativa mediante el análisis de estadísticas que advirtieron la problemática en número de casos materializados durante el 2015 en Colombia y en particular en Antioquia. Con base en lo mencionado se hizo necesario individualizar el delito de acceso abusivo descrito en el código penal Ley 1273 de 2009 artículo 269A, sin dejar de mencionar el artículo 269H de la misma ley.

Al analizar la información obtenida a través de las diferentes entidades financieras en particular de una de ellas, se encontraron las causas probables y en algunos casos el modo de operar de los ciberdelincuentes que facilitaba la comisión de fraudes a través de acceso abusivo a un sistema informático, esto hizo necesario enunciar la leyes y normas que protegen la información y los datos y que son instrumento de ayuda para la industria financiera con el fin de combatir este tipo de incidentes luego de que son llevados a cabo

3. Fase 3: Descripción de las repercusiones jurídicas asociadas a un incidente de seguridad por acceso abusivo a un sistema de información.

Con el propósito de brindar una herramienta a la industria financiera en aras de contrarrestar y mitigar el delito de acceso abusivo, se consideró necesario el enunciar las repercusiones jurídicas asociadas a un incidente de seguridad por

acceso abusivo a un sistema de información, detallando a cabalidad el bien jurídico tutelado por la ley, el tipo penal, los aspectos objetivos y subjetivos del delito de acceso abusivo y sus formas, el restablecimiento del derecho a las víctimas, la responsabilidad bancaria frente al fraude electrónico bajo la modalidad de acceso abusivo, además de las circunstancias de agravación que incrementan la pena en este delito.

4. Fase 4: Información a la comunidad acerca de los aspectos legales vinculados a un incidente de seguridad de la información en el sector financiero.

A partir de la individualización del delito de acceso abusivo y de la afectación a los bienes de la información y los datos además del patrimonio económico, se hizo necesario generar una serie de recomendaciones a la industria financiera que mitiguen el riesgo de materialización del delito de acceso abusivo y se generen acciones preventivas que proteja la información y los datos. Tales recomendaciones fueron generadas a partir del estudio de los casos analizados por medio de la dinámica de grupos en el frente de seguridad bancario y el análisis particular de 10 casos ocurridos a una de las entidades financieras estudiadas, elementos identificados que sirvieron de argumentos para alimentar dichas recomendaciones.

Es importante mencionar que a través de entrevistas realizadas a consumidores financieros se identificaron malas prácticas que facilitaron la comisión del acceso abusivo transformándolas en recomendaciones en este documento.

Teniendo en cuenta que se abordaron aspectos desde lo tecnológico y lo jurídico por medio de entrevista se identificaron buenas y malas prácticas las cuales deben ser replicadas y corregidas a la industria financiera a través de este documento.

Aprovechando las tecnologías de la información y la comunicación se decidió crear un video que de forma ilustrativa explicara el delito de acceso abusivo, las repercusiones jurídicas de este; y en este mismo también se dan a conocer algunas buenas prácticas que permitan mitigar el riesgo de ser víctima de acceso abusivo. Tratándose de las diversas generaciones que conforman a los consumidores financiero se decidió buscar un medio práctico y de fácil compresión para transmitir el mensaje, el medio de divulgación fue a través de la red social YouTube: https://youtu.be/QmqNcha54ms

5. Construcción del instructivo con las recomendaciones a partir de los enfoques tecnológico y jurídico para la mitigación del riesgo de acceso abusivo a sistemas de información en la industria financiera.

De acuerdo a la información recolectada, al análisis de la misma, al contacto con la industria financiera, la caracterización de los incidentes, las malas prácticas

identificadas, la conversación directa con algunas víctimas, la dinámica de grupos para el caso en particular frente de seguridad bancaria Medellín, la ley colombiana, las normas internacionales y el conocimiento teórico practico adquirido desde lo académico y lo laboral es como se realizó la construcción de este instructivo para la industria financiera, tomado desde los enfoques tecnológico y jurídico.

6 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

6.1 Incidentes de seguridad derivados del acceso abusivo

Para entrar en contexto y empezar a simplificar el tema del acceso abusivo es necesario conocer claramente conceptos como lo son: incidentes de seguridad y acceso abusivo. Es importante que el consumidor financiero comprenda claramente estos temas y sepa de qué manera gestionarlos o evitarlos en el momento que puedan materializarse, pues para las entidades financieras está claro en qué consisten y su tratamiento, permitiéndoles tener ventaja frente a los consumidores financieros.

Se define incidente de seguridad como: “Por Incidente de Seguridad se entiende cualquier evento inesperado o no deseado que pueda provocar una interrupción o degradación de los servicios ofrecidos por el sistema, o bien afectar a la confidencialidad o integridad de la información. Un incidente de seguridad puede ser causado por un acto intencionado realizado por un usuario interno o un atacante externo para utilizar, manipular, destruir o tener acceso a información y/o recursos de forma no autorizada. Aunque un incidente también podría ser la consecuencia de un error o transgresión (accidental o deliberada) de las políticas y procedimientos de seguridad, o de un desastre natural o del entorno (inundación, incendio, tormenta, fallo eléctrico...)”. (International Organization for Standardization/ International Electrotechnical, 2013)

En Colombia está definido el acceso abusivo a un sistema informático por el artículo 269a de la ley 1273 de enero 5 de 2009, el cual dice : El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes(Congreso de la República de Colombia, 2009a).

Teniendo en cuenta que el delito anteriormente descrito atenta contra la confidencialidad, integridad, disponibilidad de los datos y de los sistemas informáticos, y que la comisión de este se desarrolla en la internet entre otros, se requiere generar unas condiciones de seguridad que protejan la información y datos

susceptibles del acceso abusivo. Por tal motivo se hace necesario definir el término ciberseguridad: “conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan” (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015)

De acuerdo a la información recolectada mediante trabajo de campo a la sala de análisis criminal SAC de la Fiscalía General de la Nación a través del cuerpo técnico de investigación judicial CTI se encontraron las estadísticas actualizadas de algunos delitos, Figura 4, que afectan el bien jurídico de la información y los datos en Colombia, entre ellos el de acceso abusivo a sistemas informáticos y los que pueden derivarse de este. Entre estos delitos se encuentran:

DEFACEMENT (Álvarez, 2016)

Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia. El cambio de imagen puede ser a beneficio del atacante, o por mera propaganda (a beneficio del atacante o para causar una situación embarazosa al propietario de las páginas).

ESTAFA POR COMPRA VENTA DE SERVICIOS POR INTERNET

Abusar de la confianza del cliente mediante engaño en la que este no obtiene ningún beneficio pero si obtiene una pérdida económica

USURPACIÓN DE IDENTIDAD (Inteligencia Legal, 2016)

Acción por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas.

PHISING (Álvarez, 2016)

Un intento de robo de identidad en el que los delincuentes buscan conducir al usuario mediante el uso de correos electrónicos que parecen provenir de una fuente de confianza para engañar a un usuario y llevarlo a una página web falsificada con la esperanza de que revelen información privada, como nombres de usuario o contraseñas. El uso de correos electrónicos que parecen provenir de una fuente de confianza para engañar a un usuario para introducir las credenciales válidas en un sitio web falso.

SMISHING (HomeAway, 2011)

Hace referencia al *phishing* mediante mensajes cortos de celular, SMS. Al igual que en el phishing, un mensaje con un tono urgente es enviado al usuario instándolo a tomar acción. Con el *smishing* se envía un mensaje de texto al teléfono del usuario

en lugar de enviar un correo a la cuenta de correo electrónico. El mensaje de texto normalmente solicita al usuario llamar a un número de teléfono o ir a un sitio web

VISHING (HomeAway, 2011)

Ocurre cuando un estafador crea un sistema de voz automatizado para hacer llamadas a los usuarios y pedirles información privada. El propósito es el mismo que el del phishing por correo electrónico o por SMS, pues la llamada produce un sentido de urgencia en el usuario que lo lleva a tomar acción y a proporcionar información personal.

MALWARE (Instituto Nacional Español de Marketing Digital, 2015)

Es la abreviatura de Malicious software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento; dentro del grupo de Malwares podemos encontrar términos como por ejemplo, Virus, Troyanos, Gusanos (Worm), keyloggers, Botnets, Ransomwares, entre otros.

CARTAS NIGERIANAS (Álvarez, 2016)

Son una forma de estafa tradicional que empleando las nuevas tecnologías, en particular el correo electrónico, consiste en el envío de comunicaciones o cartas en las que el remitente pone a disposición del destinatario ofertas “falsas” para participar en negocios supuestamente rentables, o con la intención de involucrar a la víctima en cualquier otras situación engañosa, procurando que transfiera una fuerte cantidad de dinero para llevar a cabo la operación.

Teniendo en cuenta que el acceso abusivo no se trata de un delito común si no te tipologías especiales, realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica a partir de la consumación de este se pueden materializar otros delitos, y que en específico para la región de Antioquia se presentan ciertas modalidades, figura 7, determinadas por las estadísticas de la fiscalía general de la nación, se presentaran las definiciones de aquellas modalidades que no hayan sido definidas previamente:

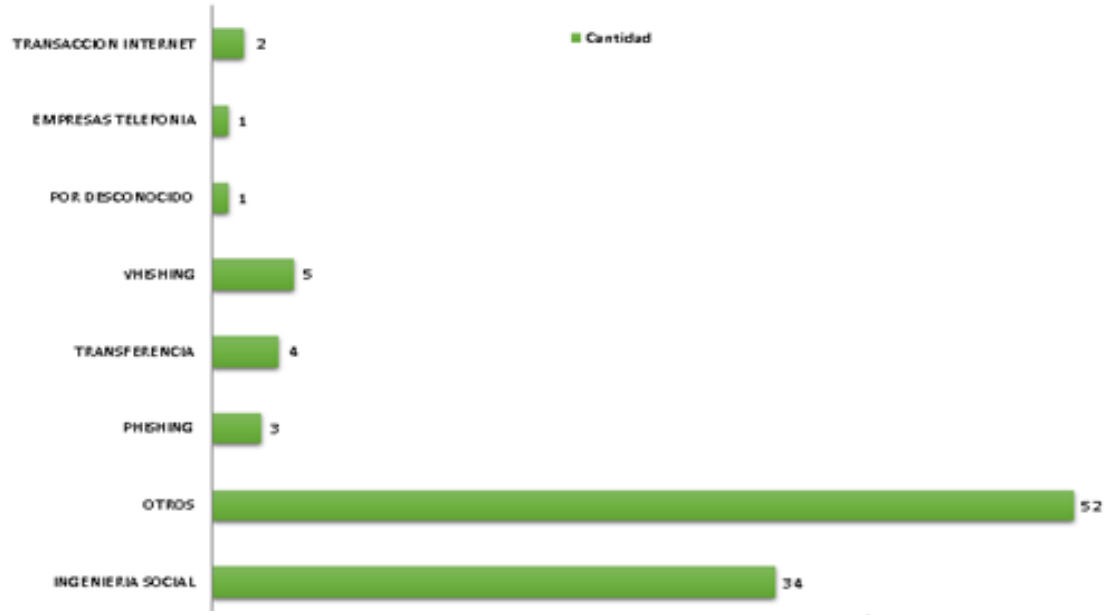


Figura 7 Delitos por acceso abusivo a sistemas de información Antioquia
Fuente: Fiscalía General de la Nación, Informe de acceso abusivo en Antioquia, 2015

TRANSACCIONES POR INTERNET (Álvarez, 2016)

Es la realización de transacciones monetarias utilizando los servicios que ofrecen la entidad o el comercio a través de internet, siendo estas no autorizadas y/o realizadas por el titular de la cuenta origen de los fondos.

EMPRESAS TELEFONICAS (Álvarez, 2016)

Se pueden dar dos modalidades para este tipo de delito:

1. Suplantación de usuarios de telefonía ante el operador para la adquisición de productos y servicios.
2. Redireccionamiento de recepción de llamadas a otras líneas telefónicas sin el consentimiento del titular de la línea

INGENIERIA SOCIAL (Álvarez, 2016)

Mecanismo para obtener información o datos de naturaleza sensible. Las técnicas de ingeniería social son técnicas de persuasión que suelen valerse de la buena voluntad y falta de precaución de los usuarios, y cuya finalidad cosiste en obtener cualquier clase de información, en muchas ocasiones claves o códigos

TRANSFERENCIA (Álvarez, 2016)

Es la transferencia no consentida de cualquier activo en perjuicio de un tercero, utilizando los portales transaccionales de las entidades financieras.

CARTAS NIGERIANAS (Álvarez, 2016)

Son una forma de estafa tradicional que empleando las nuevas tecnologías, en particular el correo electrónico, consiste en el envío de comunicaciones o cartas en las que el remitente pone a disposición del destinatario ofertas “falsas” para participar en negocios supuestamente rentables, o con la intención de involucrar a la víctima en cualquier otras situación engañosa, procurando que transfiera una fuerte cantidad de dinero para llevar a cabo la operación.

6.2 Repercusiones jurídicas asociadas a un incidente de seguridad por acceso abusivo a un sistema de información.

Tratándose de consecuencias jurídicas derivadas del acceso abusivo a sistemas informáticos es necesario comprender a cabalidad el delito en lo que se refiere a la tipicidad, antijuridicidad y culpabilidad, los bienes jurídicos que se tutelan y que se ven vulnerados por la materialización de este, el sujeto activo y pasivo, el objeto jurídico, verbo rector, aspecto subjetivo y unas conclusiones generales que adviertan y den a entender de manera clara y comprensible este delito.

Si se habla de la noción formal de delito se está haciendo referencia a que es toda conducta prevista como tal en la ley y conminada con penal. Es acción prohibida por la ley con amenaza de pena.

Los hechos para que sean punibles tienen que ser hechos del hombre, los cuales al ser hechos de los seres humanos se convierten en una conducta que solo la pueden realizar ellos, dado que el resto de seres vivos lo que realizan se denomina comportamientos, quiere decir esto que si se habla de un hecho punible tiene que ser realizado estrictamente por un ser humano, y para que sea punible es porque se realiza con punibilidad

El legislador de la ley 599 de 2000 decidió que no debería llamarse hecho punible, si no que como se explica en el párrafo anterior debe llamarse conducta punible (delitos) y que estas son típicas, antijurídicas y culpables.

Para comprender el delito del cual se está haciendo referencia es importante conocer las diferencias entre responsabilidad objetiva, derecho objetivo y objetividad jurídica.

Responsabilidad Objetiva: Es aplicar por el mero hecho o por la mera imputación.

Derecho Objetivo: Es el derecho escrito, es el derecho que está plasmado en la norma

Objetividad jurídica: Es mirar la entidad de ese bien jurídico efectivamente vulnerado

Bien: es todo lo que sea susceptible de ser valorado económica y afectivamente

Bien jurídico: Es el bien protegido por el derecho objetivo en la parte especial del código penal, ya que este es el que contempla los tipos penales , y los tipos penales protegen siempre bienes jurídicos; vale la pena aclarar que los bienes jurídicos no son solo los que están protegidos por el legislador en el código penal ya que allí están solo los más importantes, preponderancia que da el legislador en razón de la política criminal de que el derecho penal es la última “ratio” , los bienes que no están protegidos en el código penal estarán protegidos en otra norma.

Al hacer referencia a la conducta punible se debe mencionar que esta debe ser típica, antijurídica y culpable y que finalmente generara una sanción, pero que antes de decir que se impone una sanción debe haber resuelto que es responsable.

La tipicidad es diferente al tipo penal, ya que el tipo penal es aquella conducta que se encuentra objetivizada en la norma, quiere decir que la norma misma es el tipo y la tipicidad es la conducta.

La antijuridicidad puede darse de manera formal y material, la primera es que la persona con su conducta haya contrariado la voluntad del legislador y la segunda es lesionar o colocar efectivamente en peligro el bien jurídico tutelado.

La culpabilidad es el aspecto sicológico de la conducta punible ya que es propia del interior de cada persona, de este aspecto se desprende el dolo o la intención dañina, la culpa que no es más que el descuido o la negligencia y la preterintención que es el actuar con dolo buscando un resultado, pero este último va más allá del deseado

Responsabilidad: Es cuando se determina “usted realizo una conducta humana, típica, antijurídica y culpable por lo tanto es responsable y como responsable se le impone una sanción”

Comprendido lo anterior se va a analizar el delito de acceso abusivo a sistemas informáticos determinando así las repercusiones jurídicas desde la parte penal y civil.

El 5 de enero de 2009 el Gobierno Nacional sanciono la ley 1273, ley publicada en el diario oficial 47223 mediante la cual fue adicionado un nuevo título VII BIS al código penal (Ley 599 de 2001), denominado “de la protección de la información y de los datos informáticos”. Esta reforma siguió de manera parcial los estándares técnico-dogmáticos sugeridos por el convenio de Budapest del consejo de Europa de 2003 contra la cibercriminalidad.

Vale la pena mencionar que una de las figuras ampliamente modificadas por esta ley fue precisamente el delito por acceso abusivo a sistemas informáticos, tipo penal pionero en el medio jurídico colombiano que inicialmente estaba regulado por el artículo 195 del código penal capitulo VII, título III, dirigido a castigar la violación de la intimidad, reserva e interceptación de comunicaciones y que en esta oportunidad

fue incluido en el artículo 269a, dentro de las figuras que castigan especialmente “los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” que los contienen procesan o transmiten en forma automática .

El 5 de marzo de 2009 dos meses después de la ley mencionada el Gobierno Nacional sanciono la ley 1288 publicado en el diario oficial 47282, mediante la cual se expidieron normas para fortalecer el marco legal que permite garantizar la reserva de la información derivada de acciones de inteligencia y contrainteligencia que con evidente falta de planeación legislativa, revivió y modifico, en el artículo 25 el invalidado artículo 195 del código penal y derogo los artículos 4 y 269a adicionados por la reciente ley 1273 de 2009, es necesario complementar este diagnóstico manifestando que la ley 1288 de 2009 fue declarada inexequible por la corte constitucional mediante la sentencia C-913 de 2010 dejando nuevamente vigentes los artículos 4 y 269a de la ciberreforma . Más tarde el Gobierno Nacional presento de nuevo el proyecto de ley estatutaria 263 de 2011 senado y 195 de 2011 cámara de representantes fortaleciendo así el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones sancionando la ley 1621 de 2013 incorporando el articulo 40 en el que se propuso una anti-técnica modificación al código penal artículo 269a. Dicha propuesta legislativa también fue declarada inexequible por la corte constitucional en la sentencia C-540 de 2012 al quebrantar el artículo 158 de la constitución nacional, situación que mantiene incólume la vigencia actual del código penal artículo 269a.

La anterior descripción demuestra la compleja y enorme improvisación legislativa que ha rodeado la regulación de estas modalidades criminales en Colombia, la cibercriminalidad cubre aquellas conductas punibles realizadas con fines ilícitos no consentidas por el titular de la información o los datos, o abusivas de este consentimiento, que se orienta a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación, y ejecución automática de programas de datos o información informatizada reservada o secreta de naturaleza personal(privada o semiprivada), empresarial, comercial o publica, que ponga en peligro o lesionen (artículo 11 código penal) la seguridad de las funciones informáticas en sentido estricto, esto es la confiabilidad (calidad, pureza, idoneidad y corrección), la integridad y la disponibilidad de los datos o información y de los componentes lógicos de la programación de los equipos informáticos o de los programas operativos o aplicativos(software).

Lo anterior demuestra que no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos con gran riqueza técnica.

El legislador penal regulo en el código penal artículo 269A adicionado por la ley 1273 de 2009 (Congreso de la República de Colombia, 2009a) el tipo penal de acceso abusivo a sistema informático que al ser analizado desde el aspecto dogmático como lo afirma Ricardo Posada Maya en su libro Aproximación a la criminalidad informática en Colombia (Maya, 2006): " —en sentido general— se puede entender la conducta de arrogarse ilegalmente —de forma no autorizada— el derecho o la jurisdicción de intrusarse o 'ingresar' en un sistema informático o red de comunicación electrónica de datos, con la consecuente trasgresión de las seguridades dispuestas por el 'Webmaster' o prestador del servicio al 'Webhosting' u 'Owner', con el fin de proteger los servicios de transmisión, almacenamiento y procesamiento de datos que ofrece frente a posibles abusos de terceros (ingreso en cuentas de e-mail ajenas). Así como también la utilización o interferencia indebidas de dichos equipos o sistemas informáticos o telemáticos, o la permanencia contumaz en los mismos por fuera de la autorización o del consentimiento válidamente emitido por el titular del derecho (art. 32, núm. 2) o de la ley. La doctrina compara usualmente esta conducta con el delito de violación de domicilio (CP. art. 189 y ss.). No obstante, ello sería plausible si la actividad de intrusión, la permanencia contumaz o el uso ilegal se hubieren realizado de forma engañosa, clandestina o arbitraria desactivando las medidas electrónicas existentes, teniendo en cuenta que los medios a los que se accede son completamente distintos"(Cano Martínez, 2010)

6.2.1 Aspectos objetivos del acceso abusivo

Dentro del aspecto objetivo se denota el sujeto activo que a su vez es monosubjetivo y común indeterminado "el que": cualquier persona natural que realice la acción propia del tipo penal ya mencionado sin requerir alguna calificación especial, basta que sea un intruso y que se cumplan las exigencias jurídicas para ser calificado como autor . Este sujeto activo y su actuación informática pueden ser rastreados e identificados a partir de la dirección IP que ha desencadenado el ataque contra el sistema informático, acompañado del numero MAC como emisor y receptor de la información que busca concretar la acción punible. Vale la pena mencionar que este tipo penal admite la coautoría y otras formas de autoría, además de las diversas formas de participación criminal como la determinación y complicidad.

Hay que tener en cuenta que el artículo 269H de la misma ley modifica y agrava el tipo penal de la mitad a las tres cuartas partes, cuando el sujeto activo tenga las siguientes calidades:

- Servidor público en ejercicio de sus funciones, al ejecutar el acceso con abuso del cargo o de la función pública.

- Cuando el sujeto activo es considerado un *insider* responsable de la administración del sistema informático, aunque algunos doctrinantes hacen referencia a que la conducta es propia de un outsider, otros ratifican que aunque el primero de estos tenga determinada autorización para ingresar al sistema para la realización de determinadas tareas al llevar a cabo en el momento en que actué por fuera de la acordado acerca de las condiciones autorizadas resulta claramente abusivo

Si se habla de sujeto activo es necesario mencionar el sujeto pasivo el cual es común monosubjetivo y colectivo; solo pueden ser sujetos pasivos de este tipo penal aquellas personas que por una parte sean las titulares del medio informático que resulta objeto del acceso abusivo (persona natural o jurídica) y por la otra el titular de los datos personales, sensibles o secretos almacenados en archivos o bases de datos y cuya intimidad personal fue puesta en peligro. También será sujeto pasivo en sentido colectivo la comunidad como titular del bien jurídico seguridad de la información y de los datos, en particular de la seguridad de las funciones informáticas tales como la idoneidad, autenticidad y disponibilidad.

No se puede dejar a un lado el bien jurídico, en este caso tutelado por la ley 1273 de 2009. Este tipo penal pluriofensivo exige, la afectación o vulneración de bien jurídico intermedio, público y autónomo de la seguridad de la información y los datos informáticos, con lo cual se sanciona la lesión de la confiabilidad, integridad y disponibilidad directa de los sistemas informáticos y la puesta en peligro indirecto de los datos y la información almacenada en ellos.

El tipo penal exige también la puesta en peligro del bien jurídico personalismo de la intimidad personal en su modalidad de la intimidad y la autodeterminación informáticas, considerado también como un derecho fundamental de cuarta generación, buscando evitar potenciales lesiones a los datos de naturaleza privada o semiprivada y la información almacenada en el sistema objeto de ataque.

El objeto jurídico del tipo penal de acceso abusivo a sistemas informáticos consiste en proteger, en concreto, el derecho o facultad de control del titular sobre la integridad y seguridad del sistema informático, el derecho personalísimo a la autodeterminación informática y a ejercer el derecho de exclusión frente a terceros que intentan acceder de manera arbitraria, fraudulenta o violenta al sistema. Esa facultad de control se traduce en varias atribuciones concretas, susceptibles de protección:

- Requerir previa autorización o consentimiento del titular para el acceso y el uso de un sistema informático

- Saber y ser informado sobre el uso dado al sistema informático

- Orientar, corregir, excluir, etc., las condiciones de uso y el uso efectivo de un sistema informático

- El derecho a mantener protegido el sistema informático y a que nadie interfiera con dicha protección informática. Estos derechos surgen con independencia de la calidad de los datos que se encuentren almacenados en el sistema.

Independiente de donde residan los sistemas informáticos lo que corresponde a la ubicación del servidor o incluso estos pueden estar en la nube (cloud) lo importante es que el sujeto activo del tipo realice los actos de manipulación o dicte sus instrucciones intrusivas desde Colombia, para que se pueda aplicar el derecho penal nacional, lugar en el que ha iniciado la acción que produce el riesgo jurídicamente desaprobado.

El objeto sobre el cual recae la acción del acceso abusivo a sistemas informáticos, en sentido general es el sistema informático entendido como un dispositivo o grupo de dispositivos informáticos individuales interconectados entre sí que realizan acciones de tratamiento, procesamiento y almacenamiento automático de datos. En sentido estricto el objeto inmaterial sobre el cual recae la acción de acceso abusivo serían los sistemas operativos o aplicativos (software) que permiten procesar u operar automáticamente instrucciones o datos contenidos en ficheros o archivos.

La norma señala que el sujeto activo puede acceder en todo o en parte al sistema.

Finalmente vale la pena mencionar que de acuerdo al artículo 269H numeral 1, permite agravar la pena consagrada para los artículos previstos en el título, de la mitad a las tres cuartas partes cuando la acción recaiga:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

El verbo rector del artículo 269A es mixto de conducta alternativa y puede ser realizado de la siguiente manera:

a. Accediendo a un sistema informático

El acceso a sistema informático puede realizarse de manera directa, indirecta o remota lo que advierte que esta modalidad es de mera conducta y de consumación instantánea cuando se produce el acceso. El acceso tiene que ser informático o virtual no físico y se realiza mediante la digitación de comandos con los que se ordena a un sistema informático ejecutar determinada operación y esta una vez es ejecutada permite al solicitante utilizar en todo o en parte sus recursos.

Generalmente la conducta de acceso abusivo se compone de varias fases:

I. Etapa de reconocimiento: Se podría decir que en esta etapa se realizan actos preparatorios de espionaje entre los cuales se requiere conocer las características del equipo a acceder y los datos necesarios para el ingreso

II. Fase de vulneración: Esta consisten en la vulneración del sistema estructurada por los comportamientos que realmente sanciona el delito de acceso abusivo a un sistema informático, porque “implica comprometer el sistema, escalar y avanzar hasta el nivel más alto de privilegios permitido, y mantener el control del sistema atacado, o sencillamente inutilizar y generar perdida de disponibilidad del sistema bajo hostigamiento” (Cano Martínez, 2010). Actividades que usualmente son clandestinas, rápidas y para las cuales emplean programas sofisticados y técnicas de evasión y eliminación de rastros

III. Fase de eliminación y asalto: Hace referencia en anular o evadir los mecanismo de monitoreo y control, y normalizar la presencia del intruso en el sistema.

El acceso abusivo informático se denomina así por la violación de la condiciones de privacidad de la información ya que el sujeto activo carece de la autorización o del consentimiento expreso del titular del sistema informático. La conducta también será abusiva cuando el sujeto activo acceda al sistema informático en contravía de las condiciones previamente acordadas con el titular (como en el caso de existir una relación contractual, situación que también está tipificada n el numeral 2 del artículo 269H)

b. Manteniéndose en este en contra de la voluntad de quien tenga derecho a excluir.

También es una modalidad de mera conducta denominada permanencia abusiva y se da cuando el sujeto activo, si bien accede al sistema informático de manera licita o legitima, o de forma accidental o no intencional, mantiene un dialogo con el sistema informático y se mantiene conectado en contra de la voluntad concurrente del titular con derecho legítimo a excluir a los demás para proteger las condiciones de integridad, confiabilidad, disponibilidad y privacidad del medio informático.

A diferencia del verbo rector acceder, el verbo rector mantenerse es de ejecución permanente, lo que advierte que la actividad antijurídica cesa cuando el sujeto activo sale del sistema informático y termina todo tipo de dialogo abusivo, o cuando es excluido exitosamente por el sujeto pasivo.

Es necesario mencionar que es irrelevante si el sistema informático esta previamente protegido o no con una medida de seguridad informática idónea y eficaz, la eliminación de la medida de seguridad permite considerar típico un acceso a un sistema de seguridad completamente desprotegido por su titular (abierto) o con baja o reducida expectativa de intimidad, incluso por negligencia o voluntad de su dueño, siempre y cuando este no sea de acceso libre o público, o cuando no preexista un acto de autorización o consentimiento previo por parte de su dominio.

En cuanto a las repercusiones jurídicas, se castiga entonces como acceso abusivo el acceso o mantenimiento dentro de sistemas de seguridad desprotegidos, teniendo en cuanta que anteriormente antes de la creación de la ley 1273 el delito de acceso abusivo a un sistema informático se encontraba tipificado en el artículo 195 del código penal y en este la condición para acceder a un sistema informático de manera abusiva era que estuviese protegido con medida de seguridad, circunstancia que en la ley 1273 como ya se mencionó no es necesario; así con la eliminación del elemento normativo mencionado, el legislador penal dio carta abierta a la irresponsabilidad del titular, de tal manera que aunque sea diligente o negligente en la protección del sistema siempre habrá acceso punible cuando alguien ingrese a este.

El articulo 269H numerales 3 y 7 permiten modificar esta figura cuando:

a. El sujeto aproveche la confianza depositada por el dueño del sistema informático, lo que supone un mayor desvalor de acción objetivo por la forma de comisión del comportamiento (cuando el novio accede abusivamente a la cuenta de correo de su novia)

b. Cuando el sujeto realice el acceso o el mantenimiento utilizando como instrumento a un tercero de buena fe lo que supone un mayor desvalor de acción objetivo por la forma en que se facilita la comisión del delito, es de aclarar que el comportamiento sería atípico de forma absoluta cuando el sistema informático no sea de acceso restringido.

El acceso no puede ser consentido o autorizado, y si lo es, la acción del sujeto activo para ser punible, debe exceder lo acordado por las partes de manera expresa y clara, es por esta razón que la ley estatutaria 1581 de 2012 (Congreso de la República de Colombia, 2012b) en su artículo 6 especifica que “se prohíbe el tratamiento de datos sensibles, excepto cuando el titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización”.

En lo que respecta al nexo de causalidad no se requiere verificar la existencia de este ya que el tipo penal estudiado es de mera conducta. Sin embargo, en estos casos virtuales es necesario reemplazar este elemento por un nexo de naturaleza lógica que implique determinar la existencia de un dialogo informático entre el autor y el sistema informático, que obedezca a la interacción input output propiciada por las instrucciones electrónicas imputadas al sistema por el sujeto activo y respondidas por la maquina conforme al tratamiento de los datos o al software correspondiente.

La lesión a la integridad informática y el peligro para la intimidad o reserva de datos e información personal almacenada en el sistema, tienen que poder serle imputados objetivamente al sujeto activo o coautores. El acceso o el mantenimiento deben involucrar un riesgo jurídicamente desaprobado para el bien jurídico y para las

funciones informáticas de disponibilidad, integridad y seguridad de los sistemas informáticos. Así mismo, es fundamental acreditar que el intruso haya tendido el dominio del hecho sobre la introducción de las ordenas dadas al sistema operativo informático.

El riesgo informático creado debe traducirse en el resultado jurídico típico informático, esto es, la lesión a la integridad, disponibilidad y confiabilidad del sistema informático.

Con respecto a las repercusiones jurídicas del delito de acceso abusivo a sistema informático en lo que respecta al sujeto pasivo el legislador ha eliminado toda exigencia de autorresponsabilidad por parte del titular del sistema y los datos cuando no exige que el medio este protegido previamente con una medida de seguridad informática. Es irrelevante, entonces, si el titular no ha tomado medidas de protección.

6.2.2 Aspectos Subjetivos del acceso abusivo

DOLO-Articulo 22 Código Penal Colombiano (Morales, 2000)

La conducta es dolosa cuando el agente conoce los hechos constitutivos de la infracción penal y quiere su realización. También será dolosa la conducta cuando la realización de la infracción penal ha sido prevista como probable y su no producción se deja librada al azar.

Para el caso del delito de acceso abusivo en lo que se refiere al dolo se requiere que el sujeto activo conozca y quiera la realización de una conducta dirigida a acceder a todo o a una parte de un sistema informático y/o a mantenerse dentro del sistema en contra de la voluntad del titular. La conducta requiere dolo directo, pues la comisión a título de dolo eventual es extremadamente improbable.

El tipo penal de acceso abusivo a sistema informático, no exige al sujeto activo actuar con un ánimo especial o un elemento subjetivo especial distinto del dolo, que requiera la intensión de acceder al sistema informático para realizar conductas ilícitas posteriores, como, por ejemplo, el ánimo de lucro, la violación o interceptación de datos personales, el sabotaje o daños informáticos, entre otras conductas tipificadas también en la ley 1273 de 2009.

Dentro de las repercusiones jurídicas en el aspecto subjetivo también encontramos el concurso de delitos que para el caso del acceso abusivo generalmente antes de este ser ejecutado es común advertir, por ejemplo, como los criminales crean y suplantan sitios web para capturar datos personales como passwords o claves (artículo 269G código penal, subsidiario cuando no exista un delito sancionado con pena más grave), usan software malicioso (artículo 269E código penal) o violan

datos personales contenidos en ficheros, bases de datos o medios semejantes, mediante conductas de obtención, sustracción, intercambio, compra o interceptación de datos (artículo 269F y C código penal), que luego se emplean para acceder al sistema informático atacado(artículo 269A código penal).

Luego del acceso abusivo o del mantenimiento doloso también se pueden llevar a cabo otras actividades ilícitas como violaciones o interceptaciones de datos, conductas de obstaculización ilegitima del sistema (artículo 269B código penal), daños informáticos (artículo 269D código penal), transferencia no consentida de archivos y hurtos por medios informáticos entre otros. Así, en el caso de violación de datos sea previa al acceso o al mantenimiento abusivo se podría configurar un concurso efectivo de tipicidades. Por el contrario, si el acceso es previo a la violación y no se ponen en peligro bienes jurídicos diferentes a los de los sujetos pasivos , en principio, la violación de datos subsumirá materialmente (delito medio a delito fin) el acceso abusivo, aunque no faltaran autores que crean que el acceso o el mantenimiento consumado constituyen una tentativa de violación de datos personales, cuando no se logre consumar alguno de los verbos rectores previstos en la norma que requieran un resultado material.

Finalmente el delito de acceso abusivo a sistema informático previsto en el artículo 269A del código penal no es un delito común, es un cibercrimen caracterizado por exigir especiales formas y métodos de ejecución propiamente informáticos, contra sistemas informáticos, realizado por sujetos que usualmente tienen perfiles criminológicos muy precisos. Su interpretación siempre gira en torno al bien jurídico autónomo (colectivo-individual) definido como la seguridad, disponibilidad, integridad de la información, los datos y los sistemas informáticos.

Poder sancionar actuaciones sin alguna finalidad especifica permite tipificar los casos, en principio inofensivos, de hacking blanco realizado por adolescentes o por personas que solo buscan, por motivos intelectuales o por el simple reto, desafiar las seguridades de un sistema informático determinado.

Una vez explicados los aspectos objetivos y subjetivos del delito de acceso abusivo a continuación se presentará, tratándose de las repercusiones jurídicas de este delito, una figura indispensable para el consumidor financiero, y es precisamente el restablecimiento del derecho.

6.2.3 Restablecimiento del derecho

El restablecimiento el derecho es una figura de ordenamiento jurídico, inclusive elevada a la condición de norma rectora Articulo 14, Decreto 2700 de 1991, Articulo 21 Ley 600 del 2000 articulo 22 ley 906 de 2004.

El propósito de esta figura como su nombre lo indica es el resarcimiento de los daños causados a la víctima por algún tipo de delito, en este caso por el delito de

acceso abusivo a un sistema informático, quiere decir que las cosas deben regresar a como estaban antes de que se materializara el delito y que se restablezcan los derechos vulnerados.

Está regulado en el artículo 22 del código de procedimiento penal (Ley 906 de 2004), por lo que como se mencionó anteriormente ha sido considerado un principio rector de nuestro ordenamiento jurídico. Dentro de sus principales características esta precisamente ya mencionada principio rector de la actividad judicial pretendiendo así hacer cesar los efectos producidos por el delito y que las cosas vuelvan al estado anterior de la actividad de criminalidad, lo cual debe realizarse independientemente de la responsabilidad penal (sentencia c 060 de 2008).

Atendiendo entonces a su naturaleza de principio rector este emana del artículo 250 de la constitución nacional, desarrollándose en diferentes artículos del código de procedimiento penal, lo anterior permite comprender que independiente de la declaratoria de responsabilidad penal tampoco se ve afectada por la prescripción de las acciones penal y/o civil, pudiéndose adoptar las medidas de restablecimiento del derecho en cualquier momento, inclusive sin que exista una sentencia condenatoria (auto interlocutorio # 43641 del 15 de octubre de 2014).

En los eventos de prescripción de la acción penal, la Sala ha precisado que cuando es necesario asegurar el restablecimiento del derecho, la cancelación de los registros obtenidos de manera fraudulenta se debe mantener, «bajo la perspectiva de los fines del Estado de procurar la "vigencia de un orden justo y la preservación del derecho de propiedad privada" (artículos 1, 2 y 58, modificado por el A. L. núm. 01 de 1999 de la Constitución Política).

Adicionalmente, la Corte Suprema de Justicia ha entendido la figura del restablecimiento del derecho como una garantía intemporal e independiente, como se puede verificar en la sentencia de tutela nº 69080 (Corte Suprema de Justicia, 2013) "…el restablecimiento del derecho a favor de las víctimas, aún antes de la Ley 906 de 2004, es intemporal y en esa medida se puede realizar en cualquier momento de la actuación procesal, porque, como ahora lo señala la norma que viene de transcribirse -artículo 22-, es independiente a la declaración de responsabilidad penal; por consiguiente, para que opere plenamente, basta con que esté demostrada la materialidad de la conducta o el tipo objetivo. ¨

Otra de las características es que las medidas de restablecimiento del derecho no se agotan en la legislación penal: Sentencia 12 de junio de 1990 radicado No.3475 magistrado ponente Edgar Saavedra Rojas

Es así como, en esta Sentencia, se plantea que no es el juez civil el único que puede ordenar la cancelación de escrituras públicas y su registro, pues también lo debe hacer el juez penal a quien se ¨extiende la competencia para decidir cuestiones civiles vinculadas con el hecho punible y por lo tanto complementarias con la defensa jurídica y social del crimen¨.

Así mismo, en la Sentencia de Constitucionalidad nº 775/03 del 9 de Septiembre de 2003:

¨Sin lugar a dudas, primeramente el funcionario judicial (fiscal o juez) puede y debe adoptar las medidas pertinentes que estén en la legislación penal, tanto en lo sustantivo como en lo procedimental. Asimismo, en tanto las circunstancias fácticas y jurídicas lo ameriten, y con estricto cumplimiento del debido proceso, el funcionario judicial puede expedir providencias con fundamento en otras normas del orden jurídico y dentro de él, nunca por fuera de las normas jurídicas preexistentes al momento de dictar el acto jurídico; siendo claro que el funcionario jurídico no podrá adoptar medidas que se hallen al margen del ordenamiento jurídico¨.

Otra de las características de la figura de restablecimiento del derecho es que cuando se presenta una dicotomía entre los derechos de la víctima y los derechos de los terceros de buena fe, se da prelación a los derechos de la víctima .La corte suprema de justicia ha desarrollado este tema a través de diferentes providencias tales como:

- Auto interlocutorio de corte suprema de justicia - sala de casación penal nº 43641 de 15 de octubre de 2014).
- Auto Interlocutorio de Corte Suprema de Justicia - Sala de Casación Penal del 11 de Diciembre de 2013.
- Sentencia de Corte Suprema de Justicia - Sala de Casación Penal del 29 de Agosto de 2012
- Sentencia de Corte Suprema de Justicia - Sala de Casación Penal nº 40632 de 3 de Julio de 2013. Importante por hacer alusión a un CDT, título valor.
- Sentencia de Corte Suprema de Justicia - Sala de Casación Penal nº 39858 de 21 de Noviembre de 2012.

Además de lo anteriormente mencionado la jurisprudencia indica que la competencia para ordenar medidas de restablecimiento del derecho puede estar también en cabeza del juez de control de garantías, o del juez de conocimiento dependiendo de si la medida a adoptar es de carácter provisional o definitivo (auto interlocutorio sala de casación penal No. 40246 del 28 de noviembre de 2012).

Ahora bien, cuando tales medidas son de carácter provisional, independientemente de si son personales o reales, vgr. imposición de medida de aseguramiento sobre las personas; suspensión del poder dispositivo sobre bienes (arts. 83 y 85) (Congreso de la República de Colombia, 2012); suspensión de personerías jurídicas o cierres temporales de locales o establecimientos abiertos al público (art. 91 ibídem); medidas cautelares sobre bienes (arts. 92 a 101 del ejusdem) y suspensión de registros obtenidos fraudulentamente (art. 101 ib.), la competencia es del juez de

control de garantías; empero, si lo que se pretende es el restablecimiento pleno del derecho, conforme lo establece la sentencia C-060 de 2008, ya no con carácter provisional o transitorio, análisis que comporta juicios concretos y valorativos en punto de la materialidad de la conducta punible o del denominado tipo objetivo, lo cual puede ocurrir en la sentencia o en una decisión que ponga fin al proceso, la competencia será del juez de conocimiento.

6.2.4 La banca: servicio público y su responsabilidad

Estamos ante sujetos calificados del mercado financiero: Así, en la sentencia T 672 / 2010 (Corte Suprema de Justicia, 2010) se dijo lo siguiente:

¨La Banca, de acuerdo a la jurisprudencia constitucional, ejerce un servicio público en razón de la importancia que posee la actividad financiera en el marco de las relaciones económicas entre los distintos agentes del mercado. La captación de recursos del público y el suministro del crédito son labores indispensables para el desarrollo de múltiples actividades del conglomerado social, preeminencia que llevó al constituyente a consagrar la necesaria inspección y vigilancia estatal, junto con la necesidad de autorización previa para su ejercicio. Sobre el punto la Corte indicó:

"Ahora bien, pese a que no existe norma que de manera expresa así lo determine, en el derecho Colombiano es claro que la actividad bancaria es un servicio público, pues sus nítidas características así lo determinan. En efecto, la importancia de la labor que desempeñan para una comunidad económicamente organizada en el sistema de mercado, el interés comunitario que le es implícito, o interés público de la actividad y la necesidad de permanencia, continuidad, regularidad y generalidad de su acción, indican que la actividad bancaria es indispensablemente un servicio público.¨

El Tribunal de Medellín, Sala Civil, dentro del Radicado 05001 31 03 001 2008 00312 01. M.P. MARTHA CECILIA OSPINA PATINO:

Los bancos como instituciones intermediarias de crédito, despliegan su actividad comercial asumiendo los riesgos inherentes a la organización y ejecución de sus distintos servicios, por los cuales reciben una retribución, mediante el pago del manejo de cuentas, el uso tarjetas débito y crédito, consultas y transacciones telefónicas o por internet, expedición de extractos, pago por sobregiros, el uso de cajeros propios y de otras entidades financieras, pago de talonarios, pago de intereses a quien deposita tales dineros en la entidad bancaria o, mediante el cobro de los mismos a quienes los utilizan por adquirirlos en virtud de un crédito y demás operaciones internas.

(…) Este deber de la entidad se mantiene, en tanto que conlleva un riesgo y siendo que la entidad bancaria es la que ofrece ese servicio al realizar la captación de fondos provenientes del público, su custodia va implícita, tanto desde el punto de

vista físico, como del registro electrónico, situación que se armoniza con el deber de actuar con grado especial de diligencia en el desarrollo de las operaciones comerciales que constituyen su objeto social, pues la infracción de las normas legales o estatutarias que las gobiernan, repercutirían en el patrimonio de las personas directamente vinculadas a la respectiva operación de crédito, y también a terceros que, por rebote, pueden resultar afectados por la desatención del establecimiento bancario, en el entendido que ha incumplido los deberes y las obligaciones que les son propios

La rigurosa diligencia y cuidado exigida a los bancos no es la que se espera de un buen padre de familia, referida por tanto a los negocios propios, sino a la de un profesional que deriva provecho económico de un servicio en el que existe un interés público. El articulo 98 numeral 4 del Decreto 663 de 1993 (Estatuto Orgánico del Sistema Financiero), obliga a las instituciones financieras a "emplear la debida diligencia en la prestación de los servicios a sus clientes" lo mismo que a sus administradores el de "obrar no solo dentro del marco de la ley sino dentro del principio de la buena fe y de servicio a los intereses sociales (artículo 72).

En relación con el tema, la Corte Suprema de Justicia precisa el fundamento moderno de la responsabilidad bancaria, su recorrido normativo y jurisprudencial, en los siguientes términos:

El hecho es que el art. 191 de dicha Ley 46 de 1923 por su contexto consagra el sistema del riesgo creado: es decir, el aludido principio de que la responsabilidad por el pago del cheque falso es el riesgo normal del comercio de banco, Todo banco será responsable a un depositante por el pago que aquel haga de un cheque falso o cuya cantidad se haya aumentado'. Pero según se ha visto, el sistema legal del riesgo creado no impide que el banco pueda exonerarse de responsabilidad demostrando una culpa, malicia, negligencia o imprudencia de parte del girador o de sus empleados. Solo que la carga de la prueba de esas circunstancias corresponde darla al Banco.

"se estima que el ejercicio de la banca de depósito se equipara fundamentalmente al de una empresa comercial que, masivamente, atrae a si y asume los riesgos inherentes a la organización y ejecución del servicio de caja, luego es precisamente en virtud de este principio de la responsabilidad de empresa, cuyos rasgos objetivos no pueden pasar desapercibidos, que el establecimiento bancario asumiendo una prestación tacita de garantía, responde por el pago de cheques objeto de falsificación, ello en el entendido, se repite, que es inherente a la circulación y uso de títulos bancarios de ésta índole el peligro de falsificación, (...) y el costo económico de tener que pagarlos se compensa sin duda con el lucro que para los bancos reporta el cumulo de operaciones que en este ámbito llevan a cabo". C.S.J. S. C. Civil, Sentencia 16-06-2008. M.P. EDGARDO VILLAMIL PORTILLA. Exp. No. 11001-3103-007-1995-01394-01.

6.2.5 Responsabilidad bancaria frente al fraude electrónico bajo la modalidad de acceso abusivo.

Es importante mencionar que el fraude electrónico materializado bajo la modalidad de acceso abusivo puede referirse a los canales de distribución de los servicios financieros y/o a los medios de pago electrónicos entre ellos los portales virtuales transaccionales, cajeros automáticos en los cuales se utilizan tarjetas debido y crédito o terminales en las cuales el usuario se acredita como titular de la tarjeta para la realización de cualquier tipo de transacción o compra como lo son los datafonos de las redes credibanco visa o redeban multicolor.

Fraude electrónico es toda conducta desplegada por un tercero ajeno al titular del medio electrónico de pago, no autorizada ni consentida por este, generada a través de los diferentes canales entre estos los electrónicos y/o virtuales causando así un perjuicio para el titular.

Según Andrés Mariño el fraude electrónico se puede definir en el escenario en que "Un tercero se apropia de los datos de identificación de la tarjeta de crédito [o de cualquier medio electrónico de pago individual] y de su titular y, empleando los mismos, celebra contratos a distancia por medios electrónicos, telefónicos o telemáticos"(Mariño López, 2003)

Para que se materialice el fraude electrónico, asociado con el acceso abusivo, no necesariamente dependerá de la debida diligencia del titular del medio de pago, puesto que existen modalidades que pueden captar la información de dicho medio sin que el titular se percate de ello, ejemplo de esto es la instalación de dispositivos que capturan la información de la banda magnética en los cajeros automáticos conocidos como los skimmer.

Aun cuando el titular del medio de pago sea lo suficientemente cuidadosos en no prestar la tarjeta a otras personas y no revelar su clave , los delincuentes además del skimmer, instalan una cámara en un lugar estratégico que capture la clave del titular al momento de la utilización del cajero electrónico; luego el delincuente ya teniendo la información que reposa en la banda magnética más la clave, accederá de manera abusiva al sistema informático acreditándose como si fuese el titular, acción que derivara en otras modalidades delictivas que finalmente generaran pérdida económica para el titular.

En este caso y otros más las entidades financieras tienen varios tipos de responsabilidad como lo son: responsabilidad bancaria contractual, riesgo de la actividad bancaria derivada de la incorporación de nuevas tecnologías y responsabilidad profesional, lo anterior derivado de la actividad financiera.

Dentro del régimen tradicional se encuentra el régimen de responsabilidad subjetiva el cual se basa en la noción de culpa que hace referencia a la negligencia que

genera o permite el daño, de esta manera el mecanismo para determinar la ausencia de responsabilidad por parte del causante es la demostración de la diligencia que le es exigida, para el caso de las entidades financiaras en lo que respecta a la responsabilidad contractual seria la entidad emisora del medio de pago quien estaría en la obligación que actuó en forma diligente esto de acuerdo al Artículo 1604 del código civil, por lo que al titular de dicho medio de pago solo le corresponde afirmar que sus perjuicios se derivaron del incumplimiento contractual por parte de la entidad financiera; quiere decir que la carga de la prueba no está en cabeza del titular del medio de pago sino al emisor acreditar su diligencia, esto último en razón de que la entidad financiera es un profesional en el desarrollo de su actividad por lo que se le exige un grado máximo de diligencia.

Al hablar de responsabilidad subjetiva la entidad financiera está obligada a desarrollar actividades tendientes para brindar seguridad en las transacciones electrónicas con el mayor grado de diligencia.

Lamentablemente esta responsabilidad contractual en ocasiones en lugar de favorecer al consumidor financiero titular del medio de pago favorece a la entidad financiera, pues basta para entidad indicar que la operación fue exitosa ya que se realizó con el medio de pago y la contraseña asignada a este, principal medio de seguridad brindado por el banco; por lo que no podría considerarse un incumplimiento contractual del emisor.

Además del régimen ya mencionado encontramos el régimen de responsabilidad objetiva el cual surgió dentro del régimen ya mencionado equilibrando así las cargas probatorias ante determinadas situaciones.

El planteamiento del régimen de responsabilidad objetiva aunque sigue siendo contractual indica que la entidad financiera no se exime de responsabilidad probando la máxima diligencia, sino que además debe garantizar un resultado, esta responsabilidad se ha cimentado en las teorías del riesgo que se han estructurado ya no bajo la órbita de la responsabilidad contractual, sino de la extracontractual por el riesgo originado en la actividad desplegada por el emisor de los medios electrónicos de pago; bajo este supuesto deberá indemnizar perjuicios que se causen incluso a quien no tiene ningún tipo de relación jurídica con este. Lamentablemente en Colombia las entidades financieras en la mayoría de los casos cuando se materializan fraudes informáticos descargan toda la responsabilidad en el consumidor financiero sin ni siquiera tener los elementos materiales probatorios suficientes que demuestren dicha responsabilidad (Corte Suprema de Justicia, 2016)

El riesgo debe entenderse como la probabilidad de ocurrencia de una situación que genere un perjuicio de orden patrimonial a quien lo genera o a un tercero. (Rodríguez Zárate, 2014)

6.2.6 Teoría del riesgo

La teoría del riesgo tiene tres vertientes principales, como se indica a continuación. En primer lugar, en el escenario del riesgo creado, quien en desarrollo de una actividad genere un riesgo, está en la obligación de indemnizar los perjuicios que de este devengan sobre terceros. Aquí no entra en consideración si el agente que genera el riesgo obtiene o no provecho alguno con la actividad, sino simplemente si esta crea un riesgo. En segundo lugar, bajo la teoría del riesgo provecho, quien ejerza una actividad que genere un riesgo y obtenga de esta una utilidad, un provecho, deberá indemnizar los perjuicios que se causen y que sean derivados de tal riesgo, sin importar si obró o no en forma diligente. Finalmente, el riesgo profesional se ha considerado por la doctrina como una vertiente del riesgo provecho, de donde devino el desarrollo de la responsabilidad por accidentes de trabajo. No obstante lo anterior, se ha intentado darle un desarrollo independiente, considerando el riesgo derivado de las actividades que requieren un cierto grado de profesionalismo, como podría ocurrir con las profesiones liberales, en especial la responsabilidad médica, y otras como la actividad financiera. (Rodríguez Zárate, 2014)

No obstante a la luz del régimen de responsabilidad objetivo se infiere que no existen causales que eximen de responsabilidad a la entidad emisora del medio electrónico de pago, podría considerarse la fuerza mayor o el caso fortuito, el cual se nutre de dos elementos como lo son: la imprevisibilidad y la irresistibilidad, los cuales serían un buen argumentos para la entidad financiera obviamente sustentado en pruebas periciales, esto hace referencia al análisis forense que puede realizarse para sustentar los dos elementos ya mencionados.

6.3 Informar a la comunidad acerca de los aspectos legales vinculados a un incidente de seguridad de la información en el sector financiero.

Teniendo en cuenta que el tema que se ha venido desarrollando en cuanto a incidentes derivados del acceso abusivo a un sistema informático y sus repercusiones jurídicas, se circunscribe a la industria financiera, es necesario mencionar que las entidades como protagonistas de la relación entidad-cliente son vigiladas por la superintendencia financiera de Colombia SFC, quien a través de disposiciones desarrolladas en circulares externas obliga a las entidades al cumplimiento, garantizando así la protección al cliente, cliente potencial o usuario representados en el ya mencionado consumidor financiero.

Ante el creciente número de usuarios que requieren productos financieros, dichas medidas de protección del consumidor financiero se incrementaron, a tal punto que esta figura fue reglamentada por la Ley 1328 de 2009, la cual indica que las

decisiones adoptadas en ésta son obligatorias cuando las entidades vigiladas así lo prevean en sus reglamentos.

En este sentido, el Congreso de la República estableció que el usuario puede acudir a la protección de sus derechos, a la misma entidad vigilada, a la Superintendencia Financiera de Colombia -en su calidad de autoridad administrativa o jurisdiccional- o a los jueces competentes.

Dentro de la Ley 1328 de 2009 en el artículo 7 se describen las obligaciones especiales de las entidades vigiladas, se considera que el literal q de este articulo compila de manera general el cómo las entidades vigiladas deben evitar la materialización del delito de acceso abusivo al consumidor financiero disponiendo de los medios electrónicos y controles idóneos para bridar eficiente seguridad a las transacciones, a la información confidencial y a las redes que la contengan.

Si bien es cierto de acuerdo a lo mencionado anteriormente el consumidor financiero para la protección de sus derechos, en este caso los vulnerados por la materialización del delito de acceso abusivo a sistema informático, puede acudir a diferentes instancias, entre estas la entidad vigilada por la SFC, los jueces competentes (justicia ordinaria), el acudir a la SFC directamente trae consigo algunas garantías que puede ser beneficiosas para este, tales como:

- Jueces especializados que tienen conocimiento de la materia relacionada con el asunto en controversia.

- Proceso verbal sumario, lo que representa celeridad en la sentencia, aunque vale la pena mencionar que a partir del código general del proceso Ley 1564 de 2012 que entro en vigencia el primero enero de 2016, todo lo que era ordinario, abreviado, verbal de mayor y menor cuantía, entre otros paso a ser proceso verbal y proceso verbal sumario buscando descongestionar la justicia ordinaria.

- Descongestión en materia procesal ya que a diferencia de la justicia ordinaria, los jueces especializados como se dijo anteriormente, solo tendrán conocimiento de la materia relacionada, a diferencia de los jueces de la justicia ordinaria que conocerán de todo lo que corresponde a la materia civil.

Luego de esta breve introducción se darán a conocer a través de un video los aspectos legales vinculados a un incidente de seguridad de la información en el sector financiero, buscando que el consumidor financiero actué de forma preventiva y en el caso de materializado el incidente comprenda las implicaciones jurídico penales del mismo y las instancias a las cuales podrá acudir buscando el restablecimiento del derecho.

Enlace Video: **https://youtu.be/QmqNcha54ms**

6.4 Recomendaciones a partir de los enfoques tecnológico y jurídico para mitigar la materialización del riesgo de acceso abusivo a sistemas de información en la industria financiera

6.4.1 Recomendaciones e instrucciones generales a seguir para las entidades financieras

Cada vez que se materializa un hecho punible que afecta el sistema financiero y por ende a los clientes y usuarios que hacen parte de este, generalmente se inicia una investigación por parte de la entidad financiera con la cual el cliente tiene la relación comercial o por la autoridad competente previo denuncio de la víctima; aunque el fin de la investigación en la mayoría de los casos pretende determinar los responsables de los hechos, el consumidor financiero busca el restablecimiento del derecho tratando de recuperar el patrimonio afectado o la pérdida económica generada

En Colombia más del 50% de las empresas mantuvieron o disminuyeron los recursos asignados a evitar ataques informáticos en el 2016(Revista Dinero, 2017), por lo anterior es necesario que en especial las entidades financieras inviertan en seguridad de la información sobre todo para que además de un buen servicio, este se brinde con calidad, generando confianza y seguridad en los clientes.

A continuación se brindan una serie de pasos que deben seguir a nivel general las entidades financieras que permitirán prevenir perdidas económicas por las reclamaciones de los clientes y el riesgo legal que se derivan de estas.

Paso1

Informe a los clientes al momento de la vinculación acerca de los riesgos que se derivan de la operación financiera y de la utilización de los canales físicos, electrónicos y virtuales.

Paso 2

Capacite a los clientes de manera periódica acerca de la correcta y segura utilización de los portales financieros a través de internet, invitándoles a que cumplan con las medidas de seguridad que el banco promueve a través de diferentes medios y dejar constancia escrita de ello con la firma de quien recibió la capacitación dando a entender que comprendió a entera satisfacción.

Paso 3

Divulgue a través de diferentes medios las medidas de seguridad que el cliente debe adoptar para protegerse de las diferentes modalidades de delitos, entre estas el acceso abusivo a sistemas informáticos.

Paso 4.

Ofrezca a los clientes sistemas de autenticación fuerte y velar para que los clientes adopten dichos sistemas, evitando el acceso abusivo por personas inescrupulosas

Paso 5.

Cada vez que la entidad financiera reciba un reclamo por parte de un cliente manifestando que ha sido víctima de alguna modalidad delictiva entre estas el acceso abusivo, deberá atenderla de forma inmediata , realizando un informe que sustente la investigación elaborada con respecto a los hechos y almacenar dicha información además de la que se obtenga como resultado de la investigación, lo anterior con el objetivo de suministrarla a las autoridades o a quien la ley faculte en caso de que se requieran

Al realizar los informes que den cuenta de los eventos de seguridad previa reclamación del cliente, estos deben elaborarse en un lenguaje comprensible y no eminentemente técnico, para que tanto la autoridad competente como todos los interesados comprendan lo sucedido. Dichos informes deben contener:

- Un capitulo introductorio donde se explique qué es y cómo funciona el canal, sistema o lugar del Banco por donde ocurrió el fraude.
- A cada afirmación que se mencione se debe relacionar el elemento de sustento.
- No se debe indicar en el informe señalamientos de responsabilidad. Lo correcto es: Al parecer, presuntamente, se infiere.
- Indicar de donde se obtuvieron cada uno de los elementos materia de prueba que soportan la investigación (personas, áreas, sistemas, bases de datos, etc.).

En el caso de recolección de evidencias o elemento material probatorio por parte de la entidad financiera estas deben realizarse bajo las formalidades y procedimientos exigidos por la ley. Articulo 275 y siguientes de la ley 906 de 2004 (Congreso de la República de Colombia, 2012).

A los Log de transacciones anexado como elementos materia de prueba; se les debe realizar una breve introducción de que es y cómo se lee dicho log, así como también, tratar de imprimirlos en hoja membretada, igualmente la primera que es la presentación del log.

En el informe que elabora la entidad financiera mostrando debida diligencia, deben registrarse todas las acciones contingentes realizadas por la entidad inmediatamente se tuvo conocimiento de los hechos, encaminadas a contrarrestar el fraude materializado y la recuperación del dinero o información sustraída.

En caso de que la entidad financiera no haya sido diligente y su acción u omisión permitió la comisión del delito que termino afectando al consumidor financiero, debe detallarse en el informe de seguridad la falta de diligencia y tratar de conciliar con el consumidor restableciendo su derecho, evitando así gastos superiores al valor de la defraudación generados por sanciones y asuntos legales.

6.4.1.1 Recomendaciones e instrucciones para seguir a nivel tecnológico para las entidades financieras

Vale la pena mencionar que el desconocimiento de los objetivos de negocio que tiene cada organización ha generado que cada vez se presenten más fallas en seguridad debido a que no se cuenta con las herramientas tecnológicas, el personal y diferentes esquemas de gestión de la seguridad de la información que permitan la vigilancia y protección de toda aquella información que se considere fundamental para la organización.

Abordando la seguridad desde un punto de vista tecnológico se puede mencionar que existen diferentes herramientas, dispositivos y estrategias que permitirán monitorear y proteger los sistemas de información, estas pueden ser: Esquemas de autenticación y autorización, sistemas de detección de intrusos (IDS), herramientas de correlación de eventos como OSIM, firewalls, esquemas de hardening y análisis forense.

Las entidades financieras deberán contar con las siguientes características para fortalecer tecnológicamente sus organizaciones y de esta manera minimizar el acceso abusivo.

Paso 1

Utilice esquemas de autenticación fuerte en los que combine varios factores de autenticación, es decir, combine autenticación por medio de contraseñas con autenticación por medio de un certificado digital. En un gran porcentaje el acceso abusivo a un sistema informático se da por la falta de esquemas de autenticación fuertes que permitan corroborar que quien dice ser el cliente en realidad si lo sea, pues es muy poco el esfuerzo que se ha hecho a la hora de invertir en tecnología que permita fortalecer la identificación y posterior autenticación de los clientes de las entidades financieras.

El paradigma clásico de los sistemas de autenticación identifica tres factores fundamentales de autenticación:

1. Algo que se sabe (contraseña, PIN)
2. Algo que se tiene (un Token, un carné, un certificado digital)
3. Algo que se es (huella dactilar, iris, geometría de la mano)

La fortaleza de un sistema de autenticación se basa en la utilización de uno o varios factores de estos tres factores. Entre más factores incorpore y ofrezca para este caso específico la entidad financiera, más fortaleza tendrá el sistema de autenticación (National Institute of Standards and Technology, 2013).

Existen diversos esquemas de autenticación y autorización los cuales permiten corroborar la identidad y autenticidad de quien ingresa al sistema al igual que las actividades que están permitidas para el usuario autenticado. Estas formas de autenticación se pueden dar mediante usuarios y contraseñas fuertes, sistemas biométricos, esquemas de autenticación mediante servidores AAA (Authentication, Authorization and Accounting), Claves de un solo uso (OTP).

a. Usuarios y contraseñas fuertes

Tener una buena política de contraseña es muy importante para mantener la seguridad y la privacidad de un sistema informático además de la información contenida en él.(Alegre & García, 2011)

Para acceder a un sistema informático por lo general se utiliza un nombre de usuario y una contraseña que permiten la autenticación ante el sistema, pero es muy común que los usuarios no sean lo suficientemente precavidos a la hora de seleccionar su usuario y contraseña, pues usan información fácil de encontrar, como lo es: su nombre, fecha de nacimiento, hobbies, entre otros. Por tanto, es fundamental que a la hora de seleccionar un usuario y contraseña se tengan los siguientes requisitos:

- Nombres de usuarios con caracteres y números.
- Contraseñas que no tengan relación con la información personal y/o privada del usuario.
- Longitud mínima de la contraseña.
- Asignar caracteres especiales y alfanuméricos utilizando mayúsculas y minúsculas para las contraseñas.
- No tener escritas en ningún lugar las contraseñas, es necesario memorizarlas.

b. Sistemas Biométricos.

La biometría es la ciencia de reconocer un individuo basándose en sus características fisiológicas y/o de comportamiento. Los sistemas biométricos han sido empleados en varias aplicaciones comerciales, civiles y forenses. Entre los diferentes tipos de acceso biométrico, según la fisiología, se encuentran: la huella dactilar, escaneo de iris, escaneo de retina, reconocimiento facial, escaneo de la

geometría de la mano, entre otras, y según el comportamiento: firma personal, el comportamiento en el uso del computador, entre otras. (Guillermo & Andrade, 2012)

La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos, Figura 8, de su cara o por su voz. Obviamente aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes o sistemas Unix el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado recurso. (RedIRIS, 2002)

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándars	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo en 1997 (USD)	5000	5000	1200	2100	1000	1200

Figura 8. Métodos Biométricos
Fuente: Sistemas de autenticación biométrica (RedIRIS, 2002)

La autenticación por medio de sistemas biométricos consta de los pasos principalmente:

1. Lectura de datos.
2. Extracción de características de la muestra.

3. Comparación de la muestra con la información almacenada previamente en la base de datos.

4. Decisión.

En los sistemas biométricos se haría uso de esquemas criptográficos para el cifrado de una base de datos de patrones almacenados según el tipo de sistema biométrico, o la transmisión de las características de la muestra entre el dispositivo analizador y la base de datos.

c. Claves de un solo uso- One-time-password (OTP)

La duración de las claves que cada usuario tiene para la autenticación en un sistema informático puede ser de dos tipos:

1. Sin caducidad: los usuarios cambian las claves de acceso cuando lo deseen.

2. Con caducidad (Aging Password): las claves de acceso tienen un tiempo de vida establecido, asignado solo una para una única conexión, conocidas como claves de un solo acceso o por sus siglas en ingles OTP.

Cuando se hace uso de un OTP, el cual puede ser un dispositivo físico o una aplicación, se genera una clave única para un usuario, y cada vez que este desee autenticarse en el sistema se genera una clave nueva la cual caducara después de ser usada. Para aumentar la seguridad en el uso de estos dispositivos es necesario que antes de generar la clave para autenticación se tenga antes una clave sin caducidad para que el usuario acceso al dispositivo.

El concepto de OTP se materializó con el desarrollo de los Token criptográficos, los cuales son dispositivos físicos electrónicos portátiles que generan claves criptográficas “aleatorias” seguras cada 30-60 segundos y que están sincronizadas con el servidor del banco, solo la clave que está en ese momento en la pantalla del dispositivo servirá para autenticarse, ninguna de las anteriores servirá. La forma en que se crea cada número en pantalla obedece a funciones criptográficas fuertes, validadas por entes internacionales como la NIST (National Institute of Standards and Technology, 2013)

OTP en Colombia

Desde el año 2007 el Gobierno Nacional de Colombia a través de la Superintendencia Financiera de Colombia SFC, en aras de generar confianza y garantizar seguridad a los usuarios de los servicios financieros en la utilización de canales virtuales y electrónicos comenzó a generar estrategias de prevención en lo concerniente a temas de seguridad informática debido al aumento desmesurado de fraudes a través de la banca virtual, implementada en ese tiempo por parte de las entidades prestadoras del servicio de una manera quizá un poco desactualizada y vulnerable.

En octubre 25 de 2007 la SFC emitió la circular externa 052, en la cual instruía a las entidades sometidas a inspección y vigilancia, sobre los requerimientos mínimos de seguridad y calidad que deben atender para el manejo de información a través de los diferentes medios y canales utilizados para la distribución de productos y servicios que ofrecen a sus clientes y usuarios. A las entidades que prestan servicios de banca virtual, transacciones por internet y similares, la superintendencia exigió lo siguiente:

"Las entidades que ofrezcan la realización de operaciones por Internet deberán cumplir con los siguientes requerimientos:

Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.

Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios:

Ofrecer a sus clientes tarjetas débito y/o tarjetas crédito que manejen internamente cualquiera de los mecanismos fuertes de autenticación tales como: OTP (One Time Password), biometría, etc; dichas tarjetas deberán servir indistintamente para realizar transacciones en cajeros automáticos (ATM), en puntos de pago (POS), en Internet y en sistemas de audio respuesta (IVR)" (Revista Dinero, 2009)

El Gobierno Nacional dio un tiempo prudente para que las entidades del sector financiero realizaran sus implementaciones. La normatividad empezó a regir el 1º de enero de 2010. En noviembre del 2009 la revista Dinero Publicaba:

"En lo que resta del año, el sector financiero estará trabajando intensamente en la última fase de la adopción de las normas sobre seguridad bancaria que fueron fijadas por la Superintendencia Financiera a finales de 2007 a través de la circular 052. Y, si bien la banca lleva casi dos años mejorando sus estándares de seguridad y calidad de la información, sólo en esta tercera fase se van a hacer visibles para el público los esfuerzos que ha hecho el sector en este frente, pues ahora él actuará sobre sus oficinas, cajeros y servicio de internet.

A partir del 1º de enero de 2010, las entidades financieras deberán dotar todas sus oficinas y cajeros con cámaras de seguridad que permitan monitorear y dejar un registro fílmico de todas las transacciones realizadas durante un mínimo de seis meses, comenzar a ofrecer tarjetas inteligentes con chip a quien lo solicite y adoptar mecanismos de autenticación más robustos al momento de ingresar a internet, como token One Type Password (OTP), entre otras medidas. " (Revista Dinero, 2009)

Después del inicio del año 2010 y por varios años más, la circular 052, en desarrollo del estatuto orgánico del sistema financiero, fue el requerimiento del Gobierno

Nacional para las entidades sometidas a inspección y vigilancia del sector financiero fundamentalmente en el ámbito de la seguridad. Así, en octubre del año 2012, la Superintendencia Financiera de Colombia, basándose en la circular 052, publicó la circular 042, la cual es más estricta y detallada en cuanto a los temas de seguridad.

El vencimiento de la Circular 042 se fijó en aquella época, para el primero de abril de 2013. El Supervisor a través de dicha Circular presentó una serie de modificaciones a la circular 052 que pretendían mitigar los robos en servicios financieros en línea, por ejemplo, la reglamentación de los nuevos servicios móviles en SmartPhones, la definición de la autenticación como el conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. También se definen que los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es. (Superintendecia Financiera de Colombia, 2012)

La definición de forma clara y precisa de los mecanismos fuertes de autenticación que debería implementar el sector financiero de la siguiente manera:

“Biometría, certificados de firma digital, OTP (One Time Password), en combinación con un segundo factor de autenticación, tarjetas que cumplan el estándar EMV, en combinación con un segundo factor de autenticación, y registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizarán las operaciones, en combinación con un segundo factor de autenticación.” (Superintendecia Financiera de Colombia, 2012)

Y como lo afirma la redacción de la revista Portafolio: “No solo basta con una norma para proteger a los clientes y usuarios de los riesgos en la red, las entidades destinatarias tienen un papel fundamental al promover no solo el cumplimiento de los requerimientos mínimos, sino por el contrario que vayan más allá, y busquen el cumplimiento de estándares más robustos de seguridad que permitan consolidar a través de canales seguros y de calidad la confianza de los usuarios, confianza en la cual se fundamenta el sector.” (Revista Portafolio., 2013)

Luego de dar varios plazos, se definió entre julio y octubre de 2013 el plazo máximo de los bancos para implementar los cambios necesarios para cumplir la regulación.

En Julio de 2013 la revista Dinero publicaba:“Entre Julio y Octubre del 2013 los bancos tienen plazo para implementar un conjunto de técnicas y procedimientos que verifiquen la identidad del cliente, establecimiento y entidad… El Token ha sido un mecanismo robusto de autenticación y ha generado confianza en las transacciones electrónicas. En el último semestre ha habido un ‘boom’ de los grandes bancos por implementar aplicaciones móviles. Queremos incentivar que las entidades financieras hagan desarrollos propios, pero que no dejen la seguridad en manos de las personas que hacen las aplicaciones. Con un token, las transacciones están protegidas, y permite, sin necesidad de tener un dispositivo aparte, hacer el cambio de contraseña cada vez que se va a hacer una transacción. Las personas no tendrán que ir a la sucursal a hacer retiros y consignaciones, ‘dando papaya’ a la

delincuencia común", explicó Bryan Rozo, gerente de E-banking para la región andina de Gemalto, la empresa líder en seguridad digital." (Revista Dinero, 2013)

La mayoría de bancos del sector financiero entregan el token a sus clientes empresariales de manera obligatoria (en muchos casos no es posible que el cliente decida no recibir el token pues de lo contrario no se habilita el portal).

Incluso en países desarrollados como Suiza, los bancos entregan token a sus usuarios de banca personal sin que ellos lo soliciten, en Colombia, para la banca personal es opcional, uno puede solicitarlo a su banco.

d. Esquemas de autenticación con servidores AAA (Authentication, Authorization and Accounting)

Esquema de autenticación centralizado en donde se tiene un servidor que almacena una base de datos con los usuarios, permisos y diferentes eventos asociados con cada usuario (Valdivieso, 2015).

El sistema de control de acceso AAA se puede implementar haciendo uso de dos protocolos RADIUS y TACACS+. Ambos tienen funciones de autenticar, dar acceso a los elementos del sistema para los cuales el usuario tiene permiso y llevar a cabo un registro de los eventos realizados por el usuario durante el tiempo que estuvo autenticado en el sistema.

En Colombia por más de 20 años se ha utilizado la misma forma de autenticación para medios electrónicos o virtuales, siendo esta mediante un usuario y una contraseña, y hace muy poco algunas entidades financieras han optado por implementar esquemas adicionales a la autenticación tradicional como los es la autenticación OTP, pero en realidad todas estas formas de autenticar son susceptibles a ser vulneradas, circunstancia que sería poco probable si se implementarán de forma complementaria a la anterior esquemas de autenticación mediante sistemas biométricos haciendo uso de características perennes como lo son la huella dactilar, el iris o el reconocimiento facial.

Paso 2

Utilice en su organización firewalls físicos o de software en los que pueda establecer las políticas de seguridad acordes a las necesidades de seguridad de la organización, las cuales permitirán definir cómo será filtrado el tráfico que entre o salga de la red asociada con la organización.

Paso 3

Asegure su sistema de información haciendo uso del hardening, medidas de fortalecimiento de la seguridad, el cual consiste en eliminar todo aquello que no sea necesario al interior del sistema de información, hardware o software, impidiendo que un posible atacante aproveche estos recursos no utilizados

(servicios, puertos, usuarios, etc.) para vulnerar el sistema. Este proceso puede ser aplicado tanto a dispositivos activos (switchs, routers, firewalls) como a servidores y demás elementos que hagan parte del sistema. (Grupo Smartekh, 2012)

Paso 4

Utilice un esquema de detección de intrusos, IDS, que le permita verificar el comportamiento de los datos al interior de su sistema de información, que de acuerdo con los parámetros asociados con el IDS o algoritmo de detección utilizado por el mismo identificará los datos comprometidos que afecten la confidencialidad, integridad y /o disponibilidad de la información, generando alertas que permitirán detectar la presencia de este tipo de sucesos en el sistema de información (González, 2003).

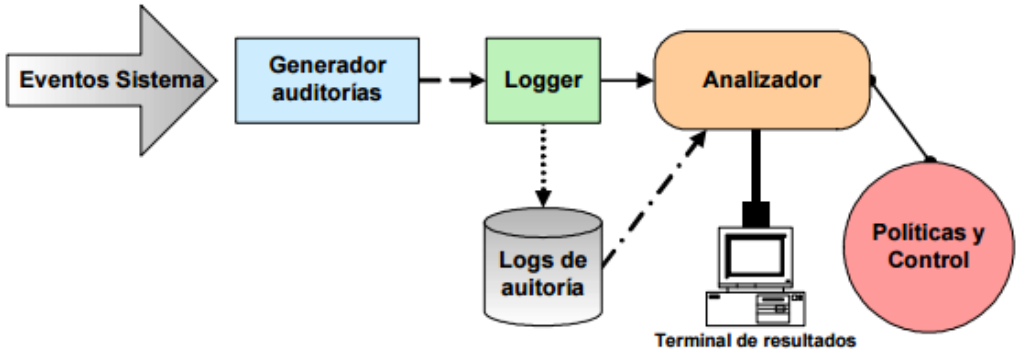


Figura 9. IDS Básico
Fuente: Sistemas de Detección de Intrusiones(González, 2003)

En la Figura 9 se muestra un sistema básico de detección de intrusos, compuesto por:

- Eventos del sistema: Son todos aquellos datos que se generan en el sistema de información
- Generador de auditoria: Toma los datos a analizar
- Log de auditoria: Datos almacenados para analizar
- Analizador: Realiza una comparación o análisis entre los datos obtenidos mediante los log y la políticas definidas para el sistema
- Políticas de Control: este campo está representado por el algoritmo de detección de intrusión, ya sea detección de anomalías (Villalba, Member, Orozco, & Vidal, 2015) o detección de mal uso. Acorde con este algoritmo serán ingresadas las políticas de seguridad
- Terminal de resultados: en este estación de trabajo se encontrará el motor de visualización de eventos del sistema en el cual se pueden ver las alarmas

generadas por el sistema así como los datos en general, ya que en ocasiones hay intrusiones que no pueden ser detectadas por el sistema, que podrían ser detectadas por el personal encargado de la administración del sistema.

Paso 5.

Utilice herramientas de correlación de eventos en su organización que le permitan tomar diferentes sucesos que ocurren al interior de su sistema de información para que estos puedan ser analizados desde diferentes enfoques, Figura 10, como los son: análisis forense, IDS, políticas de seguridad, motores de visualización (Thales, 2015). Esto con el fin de tener todas las funcionalidades integradas en un solo elemento permitiendo centralizar el control de la seguridad en el sistema de información.

Una herramienta que posee estas características es Open Source Security Information Management (OSSIM) la cual toma todos los registros obtenidos de sistema de información y los analiza acorde con las características definidas para el análisis.

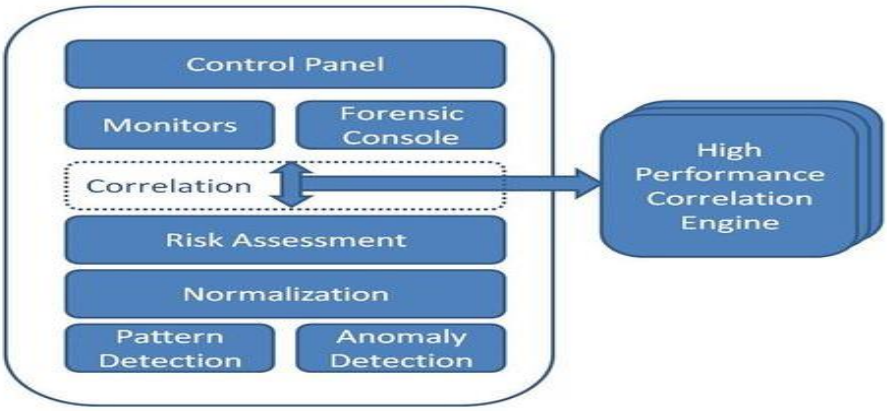


Figura 10. Herramienta de Correlación
Fuente: Fireware Security Monitoring (Thales, 2015)

Paso 6.

Implemente en la entidad el software Rapport el cual es un software de seguridad web que brinda protección en las transacciones bancarias en línea, creando un túnel de comunicación segura con los canales transaccionales un punto final del cliente; permite realizar la protección de la sesiones con cualquier sitio web que contenga información privada o personal.

Entre las funciones de este software se encuentran:

- Bloquea y congela el acceso de malware a la información sensible, incluso antes de que sea reconocido como malware.

- Notifica al cliente si se intenta acceder a un sitio web malicioso.
- Si la verificación falla Rapport termina la conexión y establece una nueva conexión.
- Realiza el cifrado de las pulsaciones del teclado y desactiva mecanismos de captura de pantalla mientras está conectado a sitios web protegidos.
- Verifica la dirección IP y el certificado SSL del sitio web cada vez que se conecta a un sitio web protegido.

Los beneficios de Rapport son:

- Remueve el malware financiera del computador.
- Se actualiza automáticamente.
- No presenta conflicto con los antivirus, por lo tanto se recomienda como complementario a este.
- No afecta el rendimiento del equipo.
- Funciona en sistemas operativos Windows y MAC OS X

Paso 7

Implemente en su organización un Sistema de gestión de seguridad de la información el cual el núcleo central son las normas ISO 27001 e ISO 27002 que establecen la forma correcta de implementar, establecer y mantener un sistema de gestión de la seguridad de la información, SGSI, aplicable para cualquier organización.

La norma ISO 27001 (International Organization for Standardization/ International Electrotechnical Commission, 2013b) establece los paramentos a tener en cuenta para la implementación de un SGSI en el que prima la confidencialidad, integridad y disponibilidad de la información; determina los entes involucrados en este proceso, así como la definición del alcance del SGSI, establecimiento de políticas para la adopción del SGSI y la evaluación de los riesgos asociados al sistema de gestión para definir el tratamiento adecuado para estos estableciendo los controles, ISO 27002, acordes a las necesidades.

En la ISO 27701 se muestran los elementos a tener en cuenta para el tratamiento de los riesgos. Lo cual implica que estos puedan ser abordados de la siguiente forma:

- Mitigados: Disminuir el riesgo, es decir implementar controles que permitan bajar el nivel del riesgo a un valor aceptable.

- Transferidos: Llevar el riesgo para que un tercero (ente exterior a la organización) le dé su debido tratamiento.
- Aceptados: Son aquellos riesgos que la organización considera que es capaz de asumir.
- Eliminarlos: Estos se da cuando es eliminada totalmente la fuente que genera este riesgo.

La norma ISO 27002 (International Organization for Standardization/ International Electrotechnical Commission, 2013a) define una serie de controles que pueden ser vistos como medidas de seguridad para el debido tratamiento de los riesgos encontrados mediante la implementación de la norma ISO 27001. Esta norma cuenta con trece dominios mediante los cuales establece las características que se deben tener en cuenta al implementar cada uno de ellos.

Paso 8

En caso de que la entidad financiera se vea involucrada en un incidente de seguridad se debe tener claro la forma en que se tiene que proceder para hacer el debido análisis de la evidencia por ello es necesario conocer cómo se hay que elaborar un análisis forense que cumpla con el rigor técnico y judicial requerido por la situación.Es necesario mencionar el término análisis forense, pues este permite realizar un análisis detallado de las diferentes acciones o procesos que se hallan llevado a cabo con dispositivos electrónicos que presuntamente se encuentran involucrados en un delito y/o delito informático. Este análisis se realiza teniendo en cuenta los siguientes pasos (Lopez, 2007) :

1. Identificación del incidente.
2. Recopilación de evidencias.
3. Preservación de la evidencia.
4. Análisis de la evidencia.
5. Documentación y presentación de resultados.

Llevar a cabo un análisis forense a manos de un experto permitirá determinar con exactitud la forma como se materializaron los hechos objeto de investigación en la maquina analizada, las circunstancias de modo, tiempo y lugar que facilitaron la comisión delictiva, las herramientas y/o malware utilizados además de las direcciones IP utilizadas para conexión a internet, esto último teniendo en cuenta que existen herramientas y métodos para enmascarar u ocultar dichas direcciones.

En el tema de la responsabilidad es necesario no solo probar el deber de diligencia en el suministro preventivo de herramientas que adviertan o impidan el acceso

abusivo como los ya mencionados IDS, sino también el mal uso o malas prácticas que realizo el usuario, consumidor financiero, que facilitaron la comisión delictiva, esto solo se demostrará con un análisis forense que dé cuenta de los eventos materializados.

La prueba técnica obtenida a través del análisis forense, aportara sustancialmente en la averiguación de responsables dentro del proceso investigativo a cargo de la autoridad competente, con el fin de judicializar a los partícipes. No obstante a partir de la Ley 1826 del 12 de enero de 2017, que comenzará a regir a parir del 12 de julio de 2017 se establece un procedimiento penal abreviado y se regula la figura del acusador privado, circunstancia que para algunos delitos de acuerdo al Artículo 534 de la citada ley la carga de la prueba puede estar en cabeza del privado.

6.4.1.2 Recomendaciones a la luz de lo reglamentado por la SFC para las entidades financieras

Recomendaciones para las entidades financieras a fin de prevenir el delito de acceso abusivo a un sistema informático entre otros a la luz de los requerimientos mínimos de seguridad y calidad para la realización de las operaciones descritos en la Circular Externa 042 del 2012 de la Superintendencia Financiera de Colombia.

Conviene revisar algunos puntos importantes, que se detallan en la Circular externa 042 del 2012 de la SFC (Superintendecia Financiera de Colombia, 2012) , con respecto a los requerimientos mínimos de seguridad y calidad que deben garantizar las entidades financieras vigiladas a sus clientes, a través de los diferentes canales que colocan a disposición de estos para la realización de las transacciones. Además del OTP (One Time Password) detallado en el numeral 2.16.3 de la circular, que hace referencia a los mecanismos de autenticación en el numeral 2.16 de la misma, es pertinente mencionar algunos numerales de la circular, al no ser tenidos en cuenta por parte de las entidades financieras que ofrecen productos y servicios al consumidor financiero pueden permitir la comisión de delitos a través de medios informáticos, entre estos el acceso abusivo a un sistema informático.

CIRCULAR EXTERNA 042 DEL 2012 (Superintendecia Financiera de Colombia, 2012)

La numeración que se muestra a continuación está relacionada con la numeración establecida por la circular externa 042 por ello no se alteraran estos valores.

2.15. Autenticación.

Conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. Los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es

2.16. Mecanismos fuertes de autenticación

Se entenderán como mecanismos fuertes de autenticación los siguientes:

2.16.1. Biometría.

2.16.2. Certificados de firma digital.

2.16.3 OTP (One Time Password), en combinación con un segundo factor de autenticación.

2.16.4. Tarjetas que cumplan el estándar EMV, en combinación con un segundo factor de autenticación.

2.16.5. Registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizarán las operaciones, en combinación con un segundo factor de autenticación.

2.17. Banca Móvil

Canal de banca electrónica en el cual el dispositivo móvil es utilizado para realizar operaciones y su número de línea es asociado al servicio.

Los servicios que se presten a través de dispositivos móviles y utilicen navegadores Web, son considerados banca por Internet.

3.1 Seguridad y calidad

3.13 Disponer que el envío de información confidencial y de los instrumentos para la realización de operaciones a sus clientes, se haga en condiciones de seguridad. Cuando dicha información se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada.

3.14 Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

3.1.6 Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada.

3.1.7 Dotar a sus terminales, equipos de cómputo y redes locales de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones

3.1.9 Ofrecer los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales realicen operaciones monetarias por los diferentes canales, siempre y cuando éstos lo permitan. En estos eventos se puede permitir que el cliente inscriba las cuentas a las cuales realizará

transferencias, registre las direcciones IP fijas y el o los números de telefonía móvil desde los cuales operará.

3.1.11Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo pueda ser realizado por personal debidamente autorizado.

3.1.13 Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación oportuna de las operaciones monetarias que no correspondan a sus hábitos.

3.3 Documentación

3.3.5 Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestarán sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información deberá ser conservada por lo menos por dos (2) años, contados a partir de la fecha de terminación de la relación contractual o en caso de que la información sea objeto o soporte de una reclamación o queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

3.4 Divulgación de información

3.4.3 Establecer las condiciones bajo las cuales los clientes podrán ser informados en línea acerca de las operaciones realizadas con sus productos.

3.4.4 Informar adecuadamente a los clientes respecto de las medidas de seguridad que deberán tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos.

3.4.5 Establecer y publicar por los canales de distribución, en los que sea posible, las medidas de seguridad que deberá adoptar el cliente para el uso de los mismos.

3.4.6 Diseñar procedimientos para dar a conocer a los clientes, usuarios y funcionarios, los riesgos derivados del uso de los diferentes canales e instrumentos para la realización de operaciones.

3.4.7 Generar un soporte al momento de la realización de cada operación monetaria. Dicho soporte deberá contener al menos la siguiente información: fecha, hora (hora y minuto), código del dispositivo (para Internet: la dirección IP desde la cual se hizo la misma; para dispositivos móviles: el número desde el cual se hizo la conexión), número de la operación, costo para el cliente o usuario, tipo de operación, entidades involucradas (si a ello hay lugar) y número de las cuentas que afectan. Se deberán ocultar los números de las cuentas con excepción de los últimos cuatro (4) caracteres, salvo cuando se trate de la cuenta que recibe una

transferencia. Cuando no se pueda generar el soporte, se deberá advertir previamente al cliente o usuario de esta situación. Para el caso de IVR y dispositivos móviles se entenderá cumplido el requisito establecido en este numeral cuando se informe el número de la operación. En relación con el costo de la operación y tratándose de cajeros automáticos, la obligación sólo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia. Tratándose de pagos inferiores a dos (2) salarios mínimos legales diarios vigentes SMLDV, no será obligatoria la generación del soporte al que se refiere el presente numeral.

4.2 Cajeros automáticos (ATM)

Los cajeros automáticos deberán cumplir, como mínimo, con los siguientes requerimientos:

4.2.2 Cuando el cajero automático no se encuentre físicamente conectado a una oficina, la información que viaja entre este y su respectivo sitio central de procesamiento se deberá proteger utilizando cifrado fuerte, empleando para ello hardware de propósito específico independiente. Las entidades deberán evaluar con regularidad la efectividad y vigencia del mecanismo de cifrado adoptado.

4.2.3 Los dispositivos utilizados para la autenticación del cliente o usuario en el cajero deben emplear cifrado.

4.2.4 Implementar el intercambio dinámico de llaves entre los sistemas de cifrado, con la frecuencia necesaria para dotar de seguridad a las operaciones realizadas.

4.2.5 Los sitios donde se instalen los cajeros automáticos deberán contar con las medidas de seguridad físicas para su operación y estar acordes con las especificaciones del fabricante. Adicionalmente, deben tener mecanismos que garanticen la privacidad en la realización de operaciones para que la información usada en ellas no quede a la vista de terceros.

4.2.6 Implementar mecanismos de autenticación que permitan confirmar que el cajero es un dispositivo autorizado dentro de la red de la entidad.

4.9 Internet

Las entidades que ofrezcan la realización de operaciones por Internet deberán cumplir con los siguientes requerimientos:

4.9.1 Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.

4.9.2 Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones monetarias por este canal. Sin embargo, cuando se

realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.

4.9.3 Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus operaciones monetarias pueda ser capturada por terceros no autorizados durante cada sesión.

4.9.4 Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.

4.9.5 Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.

4.9.6 Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

4.9.7 Contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa.

4.9.8 Las entidades que permitan realizar operaciones monetarias por este canal deben ofrecer a sus clientes mecanismos fuertes de autenticación.

4.11 Banca Móvil

El canal de Banca Móvil deberá cumplir con los siguientes requerimientos:

4.11.1 Contar con mecanismos de autenticación de dos (2) factores para la realización de operaciones monetarias y no monetarias.

4.11.2 Para operaciones monetarias individuales o que acumuladas mensualmente por cliente superen dos (2) SMMLV, implementar mecanismos de cifrado fuerte de extremo a extremo para el envío y recepción de información confidencial de las operaciones realizadas, tal como: clave, número de cuenta, número de tarjeta, etc. Esta información, en ningún caso, podrá ser conocida por los proveedores de redes y servicios de telecomunicaciones ni por cualquier otra entidad diferente a la entidad financiera que preste el servicio a través de este canal. Dicha información tampoco podrá ser almacenada en el teléfono móvil.

Cualquier comunicación que se envíe al teléfono móvil como parte del servicio de alertas o notificación de operaciones no requiere ser cifrada, salvo que incluya información confidencial.

4.11.3 Para las operaciones monetarias individuales o que acumuladas mensualmente por cliente sean inferiores a dos (2) SMMLV y que no cifren la información de extremo a extremo, la entidad deberá adoptar las medidas necesarias para mitigar el riesgo asociado a esta forma de operar, el cual debe considerar los mecanismos de seguridad en donde la información no se encuentre cifrada. La Superintendencia Financiera de Colombia (SFC) podrá suspender el uso del canal cuando se advierta que existen fallas que afecten la seguridad de la información.

5. Reglas sobre actualización de software

Con el propósito de mantener un adecuado control sobre el software, las entidades deberán cumplir, como mínimo, con las siguientes medidas:

e. Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás.

f. Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.

g. Cuando las entidades necesiten tomar copias de la información de sus clientes para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas.

h. Contar con procedimientos y controles para el paso de programas a producción. El software en operación deberá estar catalogado.

i. Contar con interfaces para los clientes o usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.

j. Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.

7. Análisis de vulnerabilidades

Las entidades deberán implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes requisitos:

a. Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

b. Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC.

c. Las entidades deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

d. Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

e. Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.

f. Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

Recomendaciones para las entidades financieras a fin de prevenir el delito de acceso abusivo a un sistema informático entre otros, a la luz de las instrucciones impartidas en la Circular Externa 052 de 2016 (Superintendecia Financiera de Colombia, 2016) de la Superintendencia Financiera de Colombia .

CIRCULAR EXTERNA 052 DE 2016 (Superintendecia Financiera de Colombia, 2016)

La numeración que se muestra a continuación está relacionada con la numeración establecida por la circular externa 052 por ello no se alteraran estos valores.

2.3.3.1.11. Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo pueda ser realizado por personal debidamente autorizado.

2.3.3.1.12. Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos.

2.3.3.1.13. Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación oportuna de las operaciones monetarias que no correspondan a sus hábitos.

2.3.3.1.14. Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales e instrumentos para la realización de operaciones. En desarrollo de lo anterior, las entidades deben establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.

2.3.3.1.15. Definir los procedimientos y medidas que se deben ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros.

2.3.3.1.16. Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se debe tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

2.3.3.1.17. Tener en operación sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.

2.3.3.1.18. Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.

2.3.3.1.19. Incluir en el informe de gestión a que se refiere el art. 47 de la Ley 222 de 1995 –modificado por el art. 1 de la Ley 603 de 2000-, un análisis sobre el cumplimiento de las obligaciones enumeradas en la presente Circular.

2.3.3.1.20. Considerar en sus políticas y procedimientos relativos a los canales de distribución, la atención a personas con discapacidades físicas, con el fin de que no se vea menoscabada la seguridad de su información.

2.3.3.1.21. Los establecimientos de crédito deben adoptar mecanismos que le permitan atender las operaciones de los consumidores financieros, por los canales que resulten necesarios y por las cuantías que determine razonables, para garantizar un nivel mínimo de prestación de sus servicios a los consumidores financieros, cuando la entidad opere fuera de línea.

2.3.3.1.22. Los establecimientos de crédito deben enviar trimestralmente a la SFC, a la dirección de correo riesgooperativo@superfinanciera.gov.co, un informe sobre la disponibilidad mensual de cada uno de los canales por medio de los cuales presta sus servicios en el que se incluya el detalle de la metodología utilizada para el cálculo de la disponibilidad. Se entiende por disponibilidad el porcentaje de tiempo que durante el mes el canal estuvo habilitado para la prestación del servicio.

2.3.3.1.23. Las entidades vigiladas deben informar a la SFC a la dirección de correo riesgooperativo@superfinanciera.gov.co, los eventos que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información manejada en los sistemas que soportan los canales de atención al cliente, haciendo

una breve descripción del incidente y su impacto. Los incidentes se deben reportar tan pronto se presenten. Así mismo, deben remitir la información de la que trata el subnumeral 3.5.1. Del Capítulo I del Título III de la Parte I de la CBJ.

2.3.3.2. En materia de documentación

Las entidades deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.3.2.1. Dejar constancia de todas las operaciones que se realicen a través de los distintos canales, la cual debe contener cuando menos lo siguiente: fecha, hora, código del dispositivo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión), cuenta(s), número de la operación y costo de la misma para el cliente o usuario.

En los casos de operaciones que obedecen a convenios, se debe dejar constancia del costo al que se refiere el presente numeral, cuando ello sea posible.

2.3.3.2.2. Velar porque los órganos de control, incluyan en sus informes la evaluación acerca del cumplimiento de los procedimientos, controles y seguridades, establecidos por la entidad y las normas vigentes, para la prestación de los servicios a los clientes y usuarios, a través de los diferentes canales de distribución.

2.3.3.2.3. Generar informes trimestrales sobre la disponibilidad y número de operaciones realizadas en cada uno de los canales de distribución. Esta información debe ser conservada por un término de 2 años.

2.3.3.2.4. Cuando a través de los distintos canales se pidan y se realicen donaciones, se debe generar y entregar un soporte incluyendo el valor de la donación y el nombre del beneficiario.

2.3.3.2.5. Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestan sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información debe ser conservada por lo menos por 2 años, contados a partir de la fecha de terminación de la relación contractual o en caso de que la información sea objeto o soporte de una reclamación o queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

2.3.3.2.6. Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal utilizado identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deben establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.

2.3.3.2.7. Llevar el registro de las actividades adelantadas sobre los dispositivos finales a cargo de la entidad, usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.

2.3.3.2.8. Dejar constancia del cumplimiento de la obligación de informar adecuadamente a los clientes respecto de las medidas de seguridad que deben tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos.

2.3.3.2.9. Grabar las llamadas realizadas por los clientes a los centros de atención telefónica cuando consulten o actualicen su información.

La información a que se refieren los subnumerales 2.3.3.2.1., 2.3.3.2.6 y 2.3.3.2.9. Debe ser conservada por lo menos por 2 años. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

6.4.2 Recomendaciones generales para los consumidores financieros

Modalidades que hacen parte de la ingeniería social a través de las cuales puede materializarse el acceso abusivo a un sistema informático:

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.(Alegre & García, 2011)

Phishing o suplantación de identidad se comente mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial y hacerse pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea. (Alegre & García, 2011)

Man in the middle (hombre en el medio) esta amenaza consiste en interceptar y modificar la comunicación entre dos equipos, con la finalidad de que el trafico pase a través del equipo que se interpone, de esta manera se captura información, contraseñas, y datos personales, además también se puede modificar esta información antes de que llegue al destinatario. (Alegre & García, 2011)

Man in the browser este es un ataque que ha evolucionado a partir del ataque Man in the middle (MITM). Es un troyano que tras infectar una maquina es capaz de modificar páginas webs, contenidos o transacciones, de una manera invisible tanto para el usuario como para el servidor web. Estos ataques son muy difíciles de detectar y además la probabilidad de que tengan éxito es muy alta ya que medidas como el SSL o cualquier otro tipo de cifrado no ayudan que este ataque desaparezca.(Alegre & García, 2011)

Trojano se denomina caballo de Troya a un software malicioso que se presenta al usuario como un programa aparentemente legitimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. (Alegre & García, 2011)

Ransomware es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.(Alegre & García, 2011)

Reexpedición de SIMCARD esta es una nueva modalidad de fraude, en la cual el delincuente se acerca al operador de telefonía móvil de su víctima con documentos falsificados, allí solicita reexpedición de la SIMCARD; vulnerando la seguridad transaccional que los bancos implementan, ya que en la actualidad para algunas transacciones se requiere la confirmación de sus transacciones mediante un dispositivo One-time-password o llamada de confirmación, y que autorizara es el delincuente que ha suplantado al titular de la cuenta.

Ahora bien conociendo estas modalidades se emiten una serie de instrucciones para que los consumidores financieros puedan mitigar el acceso abusivo a su información.

Paso 1.

Solicite a su entidad financiera completa información acerca de los riesgos a los cuales como cliente se expone cuando adquiere un producto financiero, dada la utilización de este a través de los diferentes canales (físicos, virtuales o electrónicos)

Paso 2

Pida a su entidad financiera una adecuada capacitación acerca de todas las medidas de seguridad que como cliente debe adoptar, para evitar ser víctima de delitos informáticos como el acceso abusivo. Guarde constancia de dicha capacitación.

Adopte todas las medidas de seguridad que la entidad financiera le indicó en la capacitación, mostrando deber de diligencia y cuidado con la información; lo anterior es fundamental para determinar la responsabilidad de las partes.

Paso 3

Invite a su entidad financiera a que le brinde mecanismos de autenticación fuerte, que adviertan que la conexión establecida entre cliente-banco corresponde a quien dice ser y que no se trata de un acceso abusivo.

Paso 4

Procure como consumidor financiero paramétrizar con su entidad financiera:

- Los montos de las transacciones de acuerdo a su necesidad y no deje paramétrizados montos altos de transacciones que usted nunca realizará.
- Bloquee servicios en el portal financiero que usted no va a usar
- Restrinja horarios en el portal financiero para la realización de transacciones, evitando así que personas inescrupulosas accedan a su información en horas no laborales o no habilitadas.
- En la medida de lo posible utilice una dirección IP fija y parametrizarla con la entidad financiera para el ingreso a los portales.

Paso 5.

Instalé en el equipo utilizado para realizar las transacciones bancarias software únicamente licenciado así como un antivirus reconocido y licenciado, el cual permita su actualización constantemente, así como software anti-espía licenciado como: keylogger y antispyware .

Se recomienda que este dispositivo sea únicamente utilizado para el uso de estos portales transaccionales; en la medida de lo posible el resto de la navegabilidad debe estar restringida y evitar inclusive la habilitación de buzón de correo electrónico en dicha dispositivo.

Evite descargar software de sitios web desconocidas o enlaces asociado en correos electrónicos.

Paso 6.

Defina una contraseña de entrada para su computador personal o dispositivo móvil, teniendo en cuenta que esta contraseña debe ser fuerte, para el caso que lo permita, se deben usar caracteres especiales, letras tanto mayúsculas como minúsculas, números. Si para este contraseña solo es permitido utilizar números evite el incluir información personal fácil de identificar en ellos, como fechas especiales.

Recuerde cambiar periódicamente sus contraseñas de acceso a sus dispositivos electrónicos y portales bancarios teniendo en cuenta que las contraseñas no deben

estar escritas, y siempre deben estar memorizadas para disminuir el riesgo de posible copiado de información.

No comparta usuarios y contraseñas con otras personas y en caso de que presuma o sospeche que estas han sido observadas y/o copiadas cámbielas inmediatamente memorizándolas.

Cuando no se le esté dando uso al equipo este debe permanecer apagado o bloqueado y con la debida custodia.

Paso 7.

Ingrese a sus portales financieros digitando la dirección directamente en la barra de direcciones, nunca a través de motores de búsqueda ni enlaces asociados en correos electrónicos o mensajes de texto.

Es importante que a la hora de hacer transacciones financieras por medio de sus portales financieros no se conecte a través de internet en redes públicas como: aeropuertos, hoteles, centros comerciales, café internet.

Mantenga un constante control de la plataforma transaccional, identificando conexiones exitosas e intentos de conexión fallida

No abra correos de remitentes desconocidos y mucho menos abrir archivos adjuntos, tampoco ingresar a supuestos sitios reconocidos a través de enlaces o Link.

Paso 8

Si usted realiza pagos varios a través de los portales financieros dada su actividad comercial, es importante que segregue la operación, creando a partir del usuario administrador, otros usuarios que suban, aprueben y envíen la operación; de esta manera el delincuente, requerirá las claves de todos los partícipes de la operación para realizar las transacciones fraudulentas.

El usuario administrador, solo debe ser utilizado para administrar y no para la realización de transacciones financieras, recuerde que además de que las contraseñas sean fuertes, estas deben ser diferentes para cada usuario y de exclusivo conocimiento de quien las usa.

Paso 9

Pida a su entidad financiera le sea suministrado su hábito transaccional y los registros que den cuenta de las transacciones realizadas desconocidas para usted y las cuales son objeto de investigación.

Paso 10

Tenga a la mano las líneas de comunicación inmediata con la entidad financiera para el bloqueo de sus productos en caso de que haya sido víctima de acceso abusivo u otra modalidad delictiva que afecte su patrimonio derivado de la relación comercial con la entidad financiera.

Paso 11

Inmediatamente usted evidencie que ha sido víctima de alguna modalidad delictiva que afecte su patrimonio económico derivado de la relación comercial con su entidad financiera, realice una reclamación formal ante dicha entidad y advierta de ella a instancias superiores como lo son el defensor del consumidor financiero y la SFC, además de la puesta en conocimiento a la autoridad competente mediante denuncia o querella si fuera el caso.

7 CONCLUSIONES

- Si bien es cierto al día de hoy la población de consumidores financieros en Colombia ha crecido con respecto a años anteriores, y la utilización de productos y servicios financieros ha aumentado a través de los diferentes canales que las entidades ponen a disposición de sus clientes; existe un camino muy lago por recorrer en lo que respecta a la evangelización a estos usuarios y consumidores, en cuanto a la cultura de cuidado que debe desarrollarse en especial cuando se utilizan diversos canales, minimizando de esta forma la materialización de incidentes de seguridad a través del acceso abusivo a sistemas informáticos.

- A pesar del crecimiento y desarrollo económico de nuestro país, todavía se evidencian personas jurídicas y naturales que aunque gozan de una infraestructura administrativa aparentemente robusta, se encuentran oportunidades de mejora en el manejo adecuado de la información y los datos, circunstancias que pueden facilitar la comisión de delitos como el acceso abusivo a sistemas informáticos.

- Las entidades financieras deben procurar además de ejercer la actividad propiamente financiera, dar a conocer a través de diferentes medios a sus clientes, los riesgos a los que se pueden ver expuestos en caso de mal manejo de la información, canales, productos y/o servicios.

- La gestión de los incidentes derivados del acceso abusivo a sistemas de información, deben abordarse desde tres aspectos como lo son: El técnico, el gerencial y el jurídico.

- El consumidor financiero debe adoptar todas las medidas de seguridad pertinentes para minimizar la materialización de incidentes de seguridad a través del acceso abusivo y no delegar toda la responsabilidad en la entidad financiera que pone a su disposición los diferentes canales, productos y servicios; ya que si bien es cierto a la fecha existen conceptos de las altas cortes en lo que respecta a la teoría del riesgo creado y la responsabilidad objetiva por parte de las entidades financieras, sentencia SC18614 de 2016 de la corte suprema de justicia, es necesaria la conciencia de corresponsabilidad en los protagonistas principales de este proyecto consumidor-entidad financiera, por ello las recomendaciones dirigidas a ambos.

- La industria financiera, consumidor y entidad, debe adoptar con carácter urgente las recomendaciones e instrucciones plasmadas en el presente documento, teniendo en cuenta que estas son generadas a partir de la información recolectada, el análisis de la misma, el contacto con la industria financiera, la caracterización de los incidentes, las malas prácticas identificadas, la conversación directa con algunas víctimas, la dinámica de grupos para el caso en particular frente de seguridad bancaria Medellín, la ley colombiana, las normas internacionales, la jurisprudencia y el conocimiento teórico practico adquirido desde lo académico y lo laboral.

- Las tecnologías de la información y la comunicación han facilitado el acceso a los productos, canales y servicios que brindan las entidades financieras al consumidor financiero desplazando la presencia física de estos en las oficinas a nivel nacional a un acceso a la banca virtual, sin embargo, esta circunstancia trae consigo algunos riesgos que generan pérdidas para la industria financiera de ahí la imperiosa necesidad de adoptar todas y cada una de las recomendaciones e instrucciones aquí plasmadas.

8 TRABAJOS FUTUROS

Teniendo en cuenta que el proyecto contempla una serie de recomendaciones tanto para la entidad financiera como para el consumidor financiero en lo que respecta al delito de acceso abusivo a sistemas informáticos; el próximo proyecto o trabajo derivado de los resultados de esta maravillosa experiencia, sería la escritura de un libro que compile las diferentes modalidades que afectan a los protagonistas ya mencionados y las recomendaciones para cada uno de ellos. .

9 REFERENCIAS

Alegre, M. del P., & García, A. (2011). *dise*. (Paraninfo, Ed.) (11th ed.).

Álvarez, C. (2016). CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL-POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.

APEC Telecommunications and Information Working Group. (2004). Guidelines for the Management of IT Evidence, 0–26.

Cano, J. (2015). *Computación Forense*.

Cano Martínez, J. J. (2010). *El peritaje informático y la evidencia digital en Colombia*. Universidad Los Andes.

Cissp, R. A. (2007). Información : cómo debe evolucionar la seguridad en las organizaciones ¿ QUÉ ES UN MODELO DE MADUREZ ?

Comité prevensión Fiscalia general de la Nación. Fraude en transacciones ACH (2016).

Congreso de Colombia. (1999). Ley 527 de 1999. *Diario Oficial*, 1–7. Retrieved from http://goo.gl/kYtP9D

Congreso de la República de Colombia. (2008). Ley 1266 de 2008. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Congreso de la República de Colombia. (2009a). Ley 1273 de 2009. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Congreso de la República de Colombia. Ley 1328 de 2009 (2009). Colombia. Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1328_2009.html

Congreso de la República de Colombia. (2009c). Ley 1712 de 2009. Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Congreso de la República de Colombia. (2012a). Código General del Proceso. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=48425

Congreso de la República de Colombia. (2012b). Ley 1581 de 2012. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Congreso de la República de Colombia. (2015). DECRETO 1074 DE 2015. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62508

Constituyente, A. N. (1991). *Constitución Nacional de Colombia*.

Corte Suprema de Justicia. Sentencia T 672 de 2010 (2010).

Corte Suprema de Justicia. sentencia de tutela n° 69080 del 12 de Septiembre de 2013 (2013).

Corte Suprema de Justicia. (2016). *Sentencia 18614*.

Diana, P., Prieto, B., & Peña, C. M. (1999). Evidencia Digital en Colombia : Una reflexión en la práctica.

González, D. (2003). Sistemas de Detección de Intrusiones.

Grupo Smartekh. (2012). Hardening. Retrieved from http://blog.smartekh.com/%C2%BFque-es-hardening/

Guillermo, C., & Andrade, N. (2012). Autenticación por reconcimiento facial para Aplicaciones Web.

HomeAway. (2011). ¿Qué es el smishing y el vishing?

Instituto Nacional Español de Marketing Digital. (2015). MALWARE.

Inteligencia Legal. (2016). Suplantación de Identidad. Retrieved from https://www.legalitas.com/actualidad/suplantacion-de-identidad

International Organization for Standardization/ International Electrotechnical. (2013). ISO 27035 Gestión de incidentes de seguridad de la información.

International Organization for Standardization/ International Electrotechnical Commission. (2013a). *Information technology — Security techniques — Code of practice for information security controls COPYRIGHT PROTECTED DOCUMENT*. *Iec* (Vol. 27002). Retrieved from www.iso.org

International Organization for Standardization/ International Electrotechnical Commission. (2013b). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. *Iso/Iec*. Retrieved from papers2://publication/uuid/49E9FC81-67E6-4140-B2A2-C5D8108C9F98

Jurisprudencia internacional. (2009). jurisprudencia internacional decisión 16 de diciembre 2009.

KPMG Advisory Services Ltda. (2013). Encuesta de Fraude en Colombia 2013, 37.

Lopez, M. (2007). Análisis Forense Digital.

Mariño López, A. (2003). *Responsabilidad Contractual por utilización indebida de tarjeta de crédito.* Universidad Autónoma de Barcelona.

Maya, R. P. (2006). Aproximación a la criminalidad informática en Colombia, 11–60.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). Fortalecimiento de la Gestíon TI en el Estado. Retrieved from

http://www.mintic.gov.co/gestionti/615/w3-article-2627.html

Morales, A. (2000). *Codigo Penal Ley 599 - Ley 890*. (Sexta, Ed.).

MP, M. (2012). Instituciones Financieras. Retrieved from https://educacionbancaria.wordpress.com/2012/10/26/52/

National Institute of Standards and Technology. (2013). *Electronic Authentication Guideline*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

RedIRIS. (2002). Sistemas de autenticación biométrica. Retrieved from https://www.rediris.es/cert/doc/unixsec/node14.html#SECTION055400000000000000000

Revista Dinero. (2009). Redacción Inversión. Hacia una banca más segura. *Revista Dinero*. Retrieved from http://www.dinero.com/edicion-impresa/finanzas/articulo/hacia-banca-segura/85833

Revista Dinero. (2013). Inicia la carrera tecnológica en los bancos. *Revista Dinero*. Retrieved from http://www.dinero.com/empresas/tecnologia/articulo/inicia-carrera-tecnologica-bancos/180641

Revista Dinero. (2017). Las empresas colombianas escatiman en gastos y se rajan en ciberseguridad. Retrieved from http://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201

Revista Portafolio. (2013). “Una apuesta segura para el consumidor financiero.” *Revista Portafolio.* Retrieved from http://m.portafolio.co/opinion/redaccion-portafolio/apuesta-segura-consumidor-financiero-70792

Rodríguez Zárate, A. (2014). RESPONSABILIDAD BANCARIA FRENTE A LOS FRAUDES ELECTRÓNICOS : EL RIESGO PROVECHO , EL RIESGO LAW AND ECONOMICS OF THE BANKING LIABILITY FROM ELECTRONIC FRAUDS : Para citar este artículo / To cite this article, 285–314. http://doi.org/10.11144/Javeriana.VJ128.aerb

Romo Santana, J. (2013). La prueba en el acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Sachis, C. (2011). Fraude electrónico: entidades financieras y usuarios de banca, 346.

Sección análisis criminal direccion nacional de seccionales y seguridad. (2015). Informe: Dinámica Delictiva Delitos Informáticos O.T: 45530, 8.

Soediono, B. (2000). Decreto 1747 de 2000. *Journal of Chemical Information and Modeling*, *53*, 10. http://doi.org/10.1017/CBO9781107415324.004

Superintendecia Financiera de Colombia. (2012). Circular 042, *2012*.

Superintendecia Financiera de Colombia. (2016). Circular 052.

Thales, O. B. (2015). Fireware Security Monitoring. Retrieved from https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.SecurityMonitoring

Valdivieso, A. (2015). Diseño e implementación de un sistema de autenticación y politicas de seguridad mediante un servidor AAA.

Villalba, L. J. G., Member, S., Orozco, A. L. S., & Vidal, J. M. (2015). Anomaly-Based Network Intrusion Detection System.