DESAFÍOS TÉCNICOS Y JURÍDICOS FRENTE AL CIBERDELITO EN EL SECTOR BANCARIO COLOMBIANO

BALVINA GUERRERO LOZANO
DIRLEY PIEDAD CASTILLO CAICEDO

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA - ECBTI

BOGOTÁ, D.C
2017

DESAFÍOS TÉCNICOS Y JURÍDICOS FRENTE AL CIBERDELITO EN EL SECTOR BANCARIO COLOMBIANO

BALVINA GUERRERO LOZANO
DIRLEY PIEDAD CASTILLO CAICEDO

Trabajo de grado para optar al título de Especialistas en Seguridad Informática

Director:
ANIVAR NÉSTOR CHAVES TORRES
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA - ECBTI
BOGOTÁ, D.C
2017

NOTA DE ACEPTACION

_____
_____
_____
_____

_____
JURADO

_____
JURADO

Bogotá, Septiembre 21 de 2017

Este trabajo lo dedicamos especialmente a DIOS quien es el maestro principal de todo nuestro ser.

A nuestro núcleo familiar. A nuestros hijos, parte vital, quienes nos motivan diariamente con sus resultados académicos.

AGRADECIMIENTOS

Agradecemos a nuestras grandiosas familias por el inmenso apoyo que recibimos durante toda nuestra formación como especialistas en seguridad informática. Son nuestra inspiración y el motor con el cual luchamos que nos animan continuamente para crecer como personas y como profesionales.

El presente trabajo de Grado ha sido supervisado por el ing. Anivar Néstor Chaves Torres, director del proyecto a quien deseamos darle los más sinceros agradecimientos por su apoyo, a los demás docentes de la Universidad Nacional Abierta y a Distancia UNAD por hacer posible este proyecto, su paciencia, su asesoría acertada, por sus buenos principios y siempre ese ánimo de incentivarnos a hacer las cosas con calidad.

Pero no queremos dejar sin dar gratitud al “Espíritu Santo”, porque él nos ha brindado su entendimiento y sabiduría para realizar este trabajo.

Agradecemos a los compañeros de la Universidad Nacional Abierta y a Distancia UNAD por el inmenso apoyo, amistad que nos brindaron y los grandes momentos compartidos.

Y en general a todos los que nos ayudaron a formarnos como personas íntegras enseñándonos a ser los mejores profesionales, que en el futuro aportan a una sociedad cada vez más dinámica y competitiva pero siempre con la idea clara de hacer las cosas de forma correcta.

CONTENIDO

Pág.

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

Amenazas lógicas. Bajo la etiqueta de “amenazas lógicas” se suscriben los programas que de una forma u otra pueden dañar el sistema, creados de forma intencionada para ello (software malicioso) o simplemente por error.

Ciberespacio. Se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar a excepción que la interacción en el ciberespacio no requiere del movimiento físico más allá que el de escribir.

Cracker. Es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.

Delito Informático. El delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales”. Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas.

Hacker. Es un término general que se ha utilizado históricamente para describir a un experto en programación. Recientemente, este término se ha utilizado con frecuencia con un sentido negativo, para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa, aunque no siempre tiene que ser esa su finalidad.

Seguridad activa. Se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas). Por ejemplo, utilización de contraseñas.

Seguridad física. Se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc.

Seguridad Informática. La seguridad informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Seguridad lógica. Mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.

Seguridad pasiva. Comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras). Por ejemplo, las copias de seguridad.

Tecnologías de Información. Para Gandini[1], se refieren a una rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

*UIT***.** La Unión Internacional de Telecomunicaciones UIT, es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

[1] GANDINI, Isabella. Ley de Delitos Informáticos en Colombia [en línea], 2010 [revisado 2 de marzo de 2016]. Disponible en internet:http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia.

DESAFÍOS TÉCNICOS Y JURÍDICOS FRENTE AL CIBERDELITO EN EL SECTOR BANCARIO COLOMBIANO

INTRODUCCIÓN

Globalización, sociedad de la información y la comunicación, ciberespacio, sociedad de consumo, son algunos de los calificativos con que se identifica la sociedad actual para denotar los grandes avances económicos, políticos, sociales, culturales y medioambientales. Internet y las TIC se han convertido en el principal fenómeno revolucionario que ha marcado el rumbo de una sociedad interdependiente, más comunicada, pero a su vez con grandes desafíos en materia de protección al medio ambiente, el desarrollo sustentable y el combate permanente al terrorismo y la ciberdelincuencia.

En este contexto, en la llamada sociedad de consumo, la influencia de Internet y las TIC han irrumpido con grandes progresos e impactos en el sistema financiero, especialmente los procesos de bancarización y la utilización de medios electrónicos o digitales como medios de pago que facilitan las diferentes transacciones a nivel local, regional, nacional e internacional, permitiendo la dinamización del comercio a nivel global, donde el dinero virtual y las operaciones financieras han facilitado los grandes cambios económicos, sociales y culturales de la sociedad actual.

A la par de este gran progreso tecnológico en las transacciones financieras, surgen amenazas permanentes y cada vez más sofisticadas en cuanto a la comisión de delitos informáticos, especialmente relacionados con el sistema financiero y bancario, afectando no sólo a las instituciones sino a los usuarios y cuentahabientes que hacen uso de la tecnología para sus diferentes operaciones financieras.

Frente a este fenómeno, surge la necesidad de plantear una investigación que permita establecer cuáles son los principales desafíos técnicos y jurídicos frente al delito en el sector bancario colombiano, a partir de contextualizar la tipificación del delito informático financiero y su tratamiento en el ámbito internacional por parte de algunos países y organismos especializados en esta materia.

En primera instancia, se plantea el problema, la formulación de la pregunta investigativa, los objetivos que den respuesta a la descripción y alcance de la problemática planteada con relación al ciberdelito en el sector bancario colombiano, justificando la necesidad investigativa y delimitando su alcance.

En segunda instancia, se plantea el marco de referencia donde se analizan los antecedentes que dan origen a diferentes estudios y contextualización sobre ciberdelito informático del sistema financiero y su tratamiento a la luz de la

legislación internacional y nacional dentro del marco jurídico vigente, para luego plantear el marco teórico conceptual que aborda las tecnologías de la información y la comunicación y el delito financiero, los riesgos bancarios así como el ciberdelito en el sistema financiero colombiano, para después de esto plantear la metodología relacionada con la consecución y desarrollo de esta investigación.

En tercera instancia, se presentan los resultados de la investigación en orden a los objetivos específicos planteados, cuyo cumplimiento permite dar respuesta al objetivo general y por supuesto a la pregunta de investigación. Se presenta el contexto del ciberdelito a nivel global, el tratamiento del mismo en el marco jurídico de la legislación colombiana, para luego analizar los principales desafíos técnicos que permitan luego plantear algunas estrategias para la prevención del delito informático, principalmente en el sector bancario.

El proyecto está delimitado exclusivamente a analizar las vulnerabilidades, amenazas y desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano como campo específico de tratamiento investigativo que permita la obtención de nuevo conocimiento y posibilidades de tratamiento en cuanto a su prevención y tipificación jurídico legal.

Finalmente, se plantean las principales conclusiones y recomendaciones como consecuencias del desarrollo de la investigación, un referente importante para seguir ahondando en futuras investigaciones por cuanto el tema es inagotable y la complejidad de los delitos a veces supera las acciones más sofisticadas de la institucionalidad local e internacional.

1. EL PROBLEMA DE INVESTIGACIÓN

La globalización y las transformaciones mundiales, día a día dejan ver la importancia de implementar en los sistemas informaticos metodologías para frenar el ciberdelito financiero, ya que los ciberdelincuentes encuentran brechas en las cuales les da la oportunidad para cometer el acto ilícito.

1.1 DESCRIPCIÓN

Los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en el sistema bancario en Colombia, lo cual merece un análisis de contexto sobre los principales desafíos de carácter técnico y jurídico para hacer frente al ciberdelito financiero.

Las bondades y los impactos de las TIC y el Internet en los ámbitos económico, político, social, cultural y medioambiental, han generado una serie de efectos negativos como el llamado ciberdelito o delito informático que abrió un amplio campo de riesgos y de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con la seguridad informática, la auditoría de sistemas o auditoría informática.

El desarrollo y el impacto de las Tecnologías de la Información y las Comunicaciones (TIC) han generado la concomitante necesidad de ajuste de muchas de las formas de operación y de gestión de las organizaciones, tanto de los procedimientos y estándares de las ciencias y otras tecnologías, como de la interpretación del mundo, sus culturas y paradigmas; y de esa tendencia no se excluye el Derecho, el cual debe incorporar las nuevas tendencias y formas de tipificación de delitos cometidos a través del ciberespacio, pero también la organización que debe incorporar sofisticados procesos de seguridad informática para hacer frente al ciberdelito de carácter nacional e internacional, como afirma Ojeda[2].

[2] OJEDA, Jorge Eliecer, *et al*. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. 2010. vol. 11, no. 28, p. 41-66.

Como afirma Miró[3], actualmente las organizaciones, los Estados y la comunidad internacional son beneficiarios directos de la revolución de las TIC en todos los ámbitos del quehacer humano, pero debido al tratamiento de la información, su intercambio y comunicación en la sociedad actual, también sufre los efectos negativos del cibercrimen, lo que supone que la delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas y por lo tanto, la seguridad informática en términos físicos y logísticos que deben implementar las organizaciones junto al marco jurídico de los Estados y los Organismos Internacionales, constituye una problemática que merece ser analizada y tratada de manera prioritaria.

Las organizaciones, los gobiernos y los Estados a través del Derecho y el marco jurídico de cada país, debe enfrentar no sólo a nivel interno sino a nivel global la posibilidad de frenar y castigar la comisión de delitos que afecte la relación de las personas, las organizaciones y la sociedad en general. Hay necesidad, por tanto, de regular el uso del ciberespacio con normas no sólo técnicas, ni tampoco únicamente con códigos de conducta voluntarios, sino con normas jurídicas eficaces y vinculantes que garanticen los principios y valores de los modernos ordenamientos jurídicos. También la necesidad de superar la dificultad de regular el ciberespacio, más en concreto, de tipificar penalmente las conductas que deben ser sancionadas en el ciberespacio.

Con base en Flórez[4] se puede afirmar que los nuevos retos y nuevos problemas que conlleva la existencia del ciberespacio y el Internet como medio de comunicación ha originado lo que será conocido como «ciberdelincuencia». Según Gómez[5], por su singularidad con respecto a la delincuencia tradicional, este fenómeno exige una consideración especial por parte del Derecho penal, puesto que la mayor parte de los métodos clásicos, no son los más adecuados por cuanto la diversidad de delitos cometidos en el ciberespacio, muchas veces rebasan la jurisdicción del respectivo Estado y por lo tanto hay necesidad de recurrir a la conformación de verdaderas redes inter estatales para la persecución y castigo.

Para el caso colombiano dentro del contexto de los países de la subregión, los avances significativos en términos de conectividad y utilización del Internet y las TIC, son muy significativas no sólo en el ámbito de la educación, sino también en el crecimiento de la utilización de redes sociales, el comercio electrónico y las

---

[3] MIRÓ LLINARES, Fernando. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid- España: Marcial Pons, 2012.

[4] FLORES PRADA, Ignacio. Criminalidad informática: aspectos sustantivos y procesales. Madrid-España: Tirant Lo Blanch, 2012.

[5] DIAZ GÓMEZ, Andrés. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. En: Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR. 2010. No. 8, p. 169-203.

diversas transacciones en línea, especialmente en el campo financiero. Esto ha originado, que también los delitos informáticos hayan proliferado en todas sus manifestaciones y tipificaciones, por lo tanto, le compete al Estado y las autoridades, legislar y sentar las bases para la persecución de actividades delictivas y castigar ejemplarmente a los infractores.

Por otra parte, las entidades bancarias y la implementación de verdaderos sistemas de seguridad informática, representan desafíos permanentes, dado a los avances tecnológicos y el empleo de los mismos para cometer delitos que atentan contra el patrimonio de los bancos y también de los usuarios financieros, llámese empresas o personas. Las consideraciones anteriores, constituyen referentes para plantear la necesidad de adelantar una investigación tendiente a dar respuesta a la siguiente pregunta investigativa:

1.2 FORMULACIÓN

¿Cuáles son los desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano?

1.4 OBJETIVOS

1.4.1 Objetivo General

Analizar las vulnerabilidades, amenazas y desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano.

1.4.2 Objetivos Específicos

- Contextualizar la tipificación del delito informático financiero y su tratamiento por parte de algunos países y organismos internacionales.
- Identificar el delito informático financiero cometido al sistema bancario y su tratamiento penal dentro del actual marco jurídico legal colombiano.
- Analizar la seguridad informática del sistema bancario en términos de los desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano.
- Formular recomendaciones, con base en los resultados del estudio, para la prevención del delito informático en el sector bancario colombiano.

1.5 JUSTIFICACIÓN

Las tecnología de la información y la comunicación, la cibernética y la informática representan un campo muy importante en el desempeño profesional del técnico, tecnólogo o ingeniero, convirtiéndose en un agente muy importante para garantizar la seguridad informática en las empresas y principalmente en las

entidades financieras y del sector bancario, permitiendo generar nuevos conocimiento y procesos innovadores para la detección y eliminación de riesgos no solo como permanentes desafíos de tipo técnico, sino también por las implicaciones jurídicas para hacer un solo frente en el combate a la ciberdelincuencia, lo cual conlleva a un análisis riguroso de la problemática que enfrentan las entidades financieras y también los impactos socioeconómicos para las personas afectadas por este flagelo cada vez en aumento, dado el auge y desarrollo de las TIC, las transacciones virtuales y la bancarización en línea.

El estudio monográfico desarrollado busca en primera instancia, comprender y analizar el contexto y tipificación del delito financiero en el ámbito internacional, para luego identificarlo en el caso colombiano, especialmente en el sector bancario colombiano, en términos de sus amenazas, vulnerabilidades, desafíos técnicos y jurídicos, que permitan plantear diferentes estrategias que permitan contribuir a su prevención y tipificación a la luz de la legislación vigente tanto a nivel nacional como internacional.

Desarrollar este estudio monográfico, representa una oportunidad para el fortalecimiento de una de las funciones sustantivas de educación superior: la proyección social y la intervención en el campo del ciberdelito, especialmente la estafa financiera o la movilidad de activos sin consentimiento, mediante generación de nuevo conocimiento, base fundamental para ahondar en futuras investigaciones en un campo tan complejo y cambiante como los sistemas en el contexto de una economía más globalizada.

El interés de adelantar esta investigación también obedece a la necesidad de generar estrategias de detección o prevención como un referente para adelantar futuras investigaciones en la prevención y combate al ciberdelito, especialmente el ocurrido en el campo financiero, una de las áreas de mayor crecimiento y demanda por parte de la sociedad, dada la necesidad del uso del dinero y las transacciones permanentes en un mercado globalizado.

Adelantar un proceso investigativo tipo monográfico relacionado con el ciberdelito financiero, representa un reto para el profesional en seguridad informática, por cuanto se va a poner en escena las diversas teorías, enfoques y paradigma vistos a los largo de la especialización, un análisis de la vulnerabilidad y amenazas para el sector bancario en Colombia, identificando implicaciones de tipo técnico y jurídico, una problemática latente, dado el auge del Internet y las Tecnologías de la Información y la Comunicación en todos los ámbitos de la sociedad, donde la seguridad informática debe dar una respuesta oportuna ante la tipificación de nuevos delitos en el campo financiero que afecta no solo a las instituciones bancarias sino también a los usuarios bancarizados.

2. MARCO DE REFERENCIA

2.1 ANTECEDENTES

Como se planteó anteriormente:

> La globalización y las transformaciones económicas que la explican han hecho posible la aparición, desarrollo y masificación de las nuevas tecnologías de la información. Paralelamente, el desarrollo tecnológico ha traído de la mano nuevas formas delictuales que tienen por medio o finalidad los sistemas informáticos e Internet. Las peculiaridades de estos nuevos tipos exigen un tratamiento conjunto y coherente, y del mismo modo, su problemática particular involucra elementos transnacionales, lo que obliga a la utilización de la cooperación internacional para la adopción de medidas globales[6].

Los constantes desafíos que enfrenta la sociedad y los Estados, por tanto:

> Obligan a buscar la cooperación internacional para una armonización del Derecho sustantivo, así como en el ámbito procesal, que redunde definitivamente en un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales. Para lograrlo, la cooperación internacional, que se materializa principalmente a través de convenios internacionales. El Convenio sobre la Cibercriminalidad del Consejo de Europa se presenta como una única solución internacional existente para el tratamiento de la cuestión ciberdelictual. A pesar de sus deficiencias, se convierte en una adecuada herramienta para la armonización legislativa interestatal y la lucha contra el ciberdelito[7].

Dada la proliferación de los delitos informáticos en el mundo, ha dado lugar a varias iniciativas de normativas a nivel internacional sobre delincuencia informática, las cuales datan de finales de los años 70 y surgen en el seno del Consejo de Europa. De la Conferencia auspiciada por el Consejo de Europa en 1976 sobre aspectos criminológicos de la delincuencia económica celebrada en Estrasburgo nace la primera clasificación de delitos informáticos, centrados fundamentalmente en el uso indebido de ordenadores y de programas informáticos. Ya en la década de los 80 comienza a trabajar en el Consejo de Europa una comisión de expertos dedicados al análisis de las cuestiones jurídicas relacionadas con la delincuencia informática, cuyo trabajo constituye la base de la primera recomendación del Comité de Ministros del Consejo de Europa sobre delitos informáticos[8].

---

6 FLORES PRADA. Op. Cit., p.4.

7 DIAZ GÓMEZ. Op. Cit., p. 195.

8 FLORES PRADA. Op. Cit., p.7.

Las Naciones Unidas también han tomado partido en este campo, se destacan, por una parte, instrumentos normativos genéricos producidos dentro de los trabajos de la Asamblea General. En el origen de la preocupación de Naciones Unidas por la delincuencia informática deben citarse las Resoluciones de la Asamblea General 52/91, de 12 de diciembre de 1997, 53/110, de 9 de diciembre de 1998 y 54/125, de 17 de diciembre de 1999, orientadas las tres a promocionar la organización de cursos prácticos de carácter técnico sobre análisis y prevención de la delincuencia informática, todo ello dentro de la actividad de los Congresos de Naciones Unidas sobre la Prevención del Delito y Tratamiento del Delincuente[9].

Más tarde, en las dos cumbres mundiales sobre sociedad de la información celebrada, respectivamente, en Ginebra (2003) y Túnez (2005), la Asamblea General de Naciones Unidas encomendó a la Unión Internacional de Telecomunicaciones UIT la tarea de coordinar los trabajos sobre ciberseguridad global. Fruto de este mandato, la UIT propuso en 2007 una agenda sobre seguridad informática global con siete objetivos estratégicos básicos, uno de los cuales consistía en la elaboración de propuestas normativas de bases o de modelos aplicables a la ciberdelincuencia a nivel mundial[10].

Las anteriores referencias constituyen los antecedentes en materia de buscar la armonía mancomunada de legislación para el tratamiento de delito informático en el mundo. A continuación, se presentan los antecedentes sobre este campo dado en Colombia. La Constitución Política establece normas referentes a la información y por ende se convierten en el sustento para fundar los llamados delitos informaticos. Es así que en el artículo 15 de la Carta concerniente a la intimidad de las personas y el artículo 20 relativo al derecho de información, dice:

> Artículo 15. 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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley[11].

---

9 MIRÓ LLINARES. Op. Cit.

10 FLORES. Op. Cit., p.10.

11 RODRÍGUEZ ARBELÁEZ, Juan David. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación [en línea]. 2014 [revisado 1 de marzo de 2016]. Disponible en internet: http://bdigital.ces.edu.co:8080/repositorio/handle/10946/1334.

La legislación colombiana en materia del delito informático, fue consagrada mediante la Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la Ley de Delitos Informáticos, tuvo sus propios antecedentes jurídicos. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas[12].

En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penalmente sancionatorias de las violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano: "Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones".

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:

> Artículo 192: "Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles".[13]

En cuanto a investigaciones en este campo para el caso colombiano, realmente son muy pocos, sin embargo, merece tener en cuenta la investigación realizada sobre Delitos informáticos y entorno jurídico vigente en Colombia, realizada por Ojeda donde se describe y analiza la evolución y el marco conceptual de los delitos informáticos planteados por diferentes autores nacionales e

---

12 Ibid, p. 7.

13 OJEDA, *et al*. Op. Cit., p. 18.

internacionales, y establece la relación con la reciente Ley 1273 de 2009, mediante la cual la legislación colombiana se equipara con la de otros países en cuanto a la normatividad sobre el cibercrimen, que ha venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales. Los autores plantean que el ciberdelito, como tendencia incide no sólo en el campo tecnológico sino también en el económico, político y social, el cual debe ser conocido, evaluado y enfrentado, por lo cual el análisis de la norma, su aporte y alcance puede dar otros elementos de juicio para entender la realidad de las organizaciones y visualizar sus políticas y estrategias, a la luz de la misma norma y de los estándares mundiales sobre seguridad informática.

Los antecedentes descritos a nivel internacional como nivel nacional, reflejan la importancia de un tratamiento analítico de revisión de literatura pertinente a fin de generar nuevo conocimiento para el debate, el análisis y la implementación de la seguridad informática en el sector financiero y el impacto de prevención que puede originar en los usuarios bancarizados.

2.2 MARCO TEÓRICO CONCEPTUAL

El marco teórico para esta propuesta monográfica está relacionada en primera instancia con establecer el ámbito de las tecnologías de la información y la comunicación, el Internet y la configuración de lo que hoy se denomina el ciberespacio, dentro del cual ocurren una serie de delitos que merecen ser tenidas en cuenta por la sociedad, los gobiernos y las instituciones para su persecución y castigo acorde a la legislación interna, pero también según los acuerdos internacionales, dado que en su mayoría rebasan las fronteras físicas tradicionales de los Estados. Posteriormente, se analiza la caracterización del ciberdelito en América Latina, para luego centrarlo exclusivamente en el sector financiero colombiano

2.2.1 Las TIC y el Ciberdelito

El Internet, representa en la sociedad de la información y el conocimiento una de las grandes innovaciones de los últimos años, mucho se ha escrito sobre su existencia, importancia e impacto que ha generado en la sociedad. Gómez señala que:

> La inexistencia de fronteras reales es una de las características intrínsecas de Internet, que ofrece innumerables ventajas y como no podía ser de otro modo, inconvenientes para la persecución de actividades delictivas. En primer lugar, para iniciar cualquier política criminal, hay que conocer cuál va ser el terreno de actuación. Dicho de otra manera, saber «dónde está Internet»; se está ante uno de los grandes problemas que existen, dada la dificultad de responder con exactitud a dicha pregunta. No se trata de que Internet no esté en ningún sitio, o de que esté en todos, como se suele decir. Internet no está en el aire: aun no siendo un ente físico al que estamos acostumbrados, sí está «en algún lugar». La ingente cantidad de

información que la compone está alojada en servidores distribuidos por todo el globo[14].

Para Flores con respecto a la identificación y clasificación de los diferentes delitos cometidos a través del ciberespacio, clasifica dichos delitos en dos grupos:

> El primer grupo de delitos no plantea excesivos problemas por cuanto están destinados a proteger el terminal o sus sistemas de comunicación considerados como objeto material, esto es, la integridad del terminal, de sus componentes o del sistema de conexiones respecto del uso inconsentido, de los daños que pudieran sufrir, o de su sustracción. Respecto de ellos, únicamente cabe decidir si los ataques físicos a los terminales y a los sistemas de comunicación, su uso inconsentido, o su sustracción, deben tipificarse expresamente como delitos especiales, o basta con la protección genérica que los códigos penales dispensan a la propiedad o a la integridad de los bienes. El segundo grupo es considerablemente más complejo de definir, ya que la utilización de los ordenadores, sistemas informáticos, dispositivos o redes de comunicaciones digitales con fines delictivos abre un amplio abanico de conductas susceptibles de lesionar distintos bienes jurídicos. Por una parte, conviene tener en cuenta que numerosas conductas delictivas pueden emplear los sistemas informáticos como medio o instrumento de comisión, sin que ello modifique o influya en la descripción genérica de la conducta ni que, por tanto, sea precisa una tipificación expresa[15].

Ahora bien, el auge del Internet y las tecnologías de información y la comunicación deben contextualizarse en el marco de la globalización económica, social, política, cultural y medioambiental. Las bondades de la globalización y el ciberespacio en general, encierran también peligros permanentes como la proliferación de la ciberdelincuencia que afecta a las personas, las organizaciones, los gobiernos y la comunidad internacional en general. Así:

> Los acelerados procesos de globalización con sus innumerables y cada vez más sorprendentes atractivos y posibilidades para la humanidad entera, impulsados todos por el avance tecnológico de las comunicaciones y la informática se han convertido en el nuevo paradigma de las relaciones personales, organizacionales, locales e internacionales, del conocimiento y el desarrollo. Pero tan importante y dinámico cambio que ha condicionado los nuevos comportamientos sociales, económicos, políticos y éticos de las personas y los pueblos, ha venido acompañado de un no menos dinámico y, a la vez, peligroso proceso de una nueva delincuencia que, al utilizar o impactar los sistemas de información y comunicación de las organizaciones y el mundo, ha llegado a posicionarse como uno de los cada vez mayores peligros para la seguridad, la honra, vida y bienes de las personas y las organizaciones de todos los países[16].

---

14 DIAZ GÓMEZ. op. Cit., p. 22.
15 FLORES. Op. Cit., p.15.
16 OJEDA, *et al*. Op. Cit., p. 66.

Frente a la globalización y el ciberespacio donde también se puede decir que se dan los fenómenos de masificación de la tecnología, la información y las comunicaciones, lo cual ha permitido el desarrollo y el progreso de la humanidad, son aspectos eminentemente positivos que merecen destacarse en el contexto de la sociedad de la información y la comunicación, pero también está el aspecto negativo, que junto al progreso y la globalización también prolifera la ciberdelincuencia, lo cual ha llevado a las organizaciones y algunos gobiernos del mundo a tomar mayor conciencia de la perspectiva de futuro y la subyacente amenaza, y por tanto:

> Para actuar mancomunadamente y construir barreras no sólo tecnológicas, sino también jurídicas y sociales que permitan enfrentar con probabilidades de éxito ese gran mapa de riesgos generado por los delitos informáticos. Como consecuencia, se han diseñado, divulgados y aplicados no sólo modelos, sistemas, herramientas y procedimientos de seguridad informática, sino también el necesario complemento legal para combatir el delito, además de la capacitación y preparación especializada para manejar estos componentes de seguridad, de manera integrada y cada vez más generalizada entre la sociedad[17].

He aquí la importancia del ciberdelito como los problemas que aquejan a la humanidad, a los gobiernos de los países en general, un desafío permanente para las ciencias políticas y el derecho de cada nación.

2.2.2 Riesgos Bancarios en América Latina

Según artículo publicado por la Agencia EFE:

> El 98,5 % de los riesgos bancarios en América Latina y el Caribe son digitales o informáticos, según un estudio de la Federación Latinoamericana de Bancos - FELABAN- presentado en Panamá. “Los robos en las oficinas bancarias, los asaltos a mano armada, han pasado a ser el 1,5 % del problema. Antes el riesgo era físico y patrimonial (...) Hoy en día, el riesgo es digital, informático”, indicó el secretario general de la FELABAN, Giorgio Trettenero. Esto se explica principalmente porque las nuevas tecnologías han transformado el sector financiero y han provocado, entre otras cosas, que los jóvenes “ya no vayan a las oficinas bancarias y quieran hacerlo todo por el iPad, por los teléfonos”, apuntó Trettenero[18].

El informe de la FELABAN fue presentado durante el XXX Congreso Latinoamericano de Seguridad Bancaria, que se celebró en la capital panameña. Los bancos de América Latina enfrentan tres riesgos informáticos principales:

---

17 OJEDA, *et al*. Op. Cit., p. 66.

18 AGENCIA EFE. El 98,5 por ciento de los riesgos bancarios en América Latina son informáticos [en línea]. 15 de octubre de 2015 [revisado el 2 de marzo de 2016]. Disponible en internet: https://www.efe.com/efe/america/economia/el-98-5-por-ciento-de-los-riesgos-bancarios-en-america-latina-son-informaticos/20000011-2738875 .

- La clonación de tarjetas.
- La suplantación de identidad en compras no presenciales.
- El Phishing.

Este último término se utiliza para describir un modelo de abuso informático en el que un ciberdelincuente se hace pasar por una persona o una institución de confianza para obtener información confidencial del cliente de forma fraudulenta, por lo tanto, la incorporación de estrategias para minimizar riesgos como la tecnología chip en las tarjetas de débito y crédito y el uso en las compras online de "*token de seguridad*", un dispositivo electrónico que usan los clientes para validarse, son entre otros algunos de los avances de la industria financiera para combatir el ciberdelito[19].

2.2.3 Ciberdelito en el sistema financiero colombiano

Encontramos en la revista Portafolio que:

> A medida que los usuarios del sistema financiero colombiano han venido accediendo con más facilidad durante los últimos años a medios digitales (como teléfonos inteligentes, tabletas y ordenadores personales) para realizar transacciones en línea, las posibilidades para que los delincuentes cometan fraudes en línea en Colombia parecen tornarse cada vez más fuertes. Esta es una de las advertencias que lanzó ASOBANCARIA (el gremio de la banca) el cual señaló –con cifras de la Fiscalía General de la Nación como soporte– que las denuncias por ciberdelincuencia aumentaron un 25 por ciento en el primer semestre de este año[20].

Según informes de la Fiscalía General de la Nación, tan solo en el primer semestre del 2015 el número de denuncias por ese delito asciende a 6.633. “El 75 por ciento de los delitos reportados entre el 2009 y el 2015 se asocian con el sistema financiero”. La tasa de delitos informáticos en el país viene creciendo más rápido que lo visto en fenómenos como el narcotráfico y los homicidios. Es necesario replantear la concepción que se tiene del derecho penal para poder entender este fenómeno para enjuiciar a personas de bandas dedicadas a delitos informáticos[21].

Más adelante encontramos que:

> Una buena parte de los fraudes que se dan en el sistema financiero colombiano, explica Gina Pardo, directora de gestión operativa y de seguridad de

---

19 Ibid, p. 1

20 PORTAFOLIO. Denuncias de Ciberdelitos crecen Al 25 % en Colombia, octubre 30 de 2015 [revisado 3 de abril de 2016). Disponible en internet: http://www.portafolio.co/economia/finanzas/denuncias-ciberdelitos-crecen-25-colombia-26308

21 Ibid, p. 1

> ASOBANCARIA, no se presenta a través de mecanismos sofisticados sino de correos y aplicaciones móviles. “Es la manera para hurtar información financiera que es empleada para robar. Las pérdidas por las denuncias que refieren las autoridades son cercanas a los $80.000 millones”. A pesar de que se usan métodos que en apariencia no son complejos, dado que detrás de los delitos informáticos en el país se esconden estructuras delincuenciales organizadas a las que las autoridades deben perseguir y enjuiciar[22].

ASOBANCARIA señaló que un estudio de la Organización de Estados Americanos (OEA) y Symantec:

> Advierte que el fraude cibernético en Colombia es un fenómeno equivalente a US$461 millones cada año. En países como Brasil, ese flagelo le cuesta a la economía US$8.000 millones y en México, US$3.000 millones. Todo el sistema financiero invierte muchos recursos cada año en tecnología para realizar transacciones. Los bancos siguen implementando medidas de seguridad, pero también los clientes tienen la obligación de cuidar más las herramientas que la banca da como medio de pago para evitar el ciberdelito. ASOBANCARIA sostiene que los clientes son los eslabones más débiles de la cadena. El 30 por ciento de los ataques se da contra personas naturales y un 70 por ciento, contra las compañías, según investigaciones sobre ese fenómeno muestran que los delitos informáticos tienen en ocasiones origen en naciones donde la legislación frente a la ciberpiratería es débil. En el 2011 se expidió un CONPES de ciberseguridad y ciberdefensa. No obstante, pese a los avances, los desafíos son enormes[23].

2.3 MARCO CONTEXTUAL

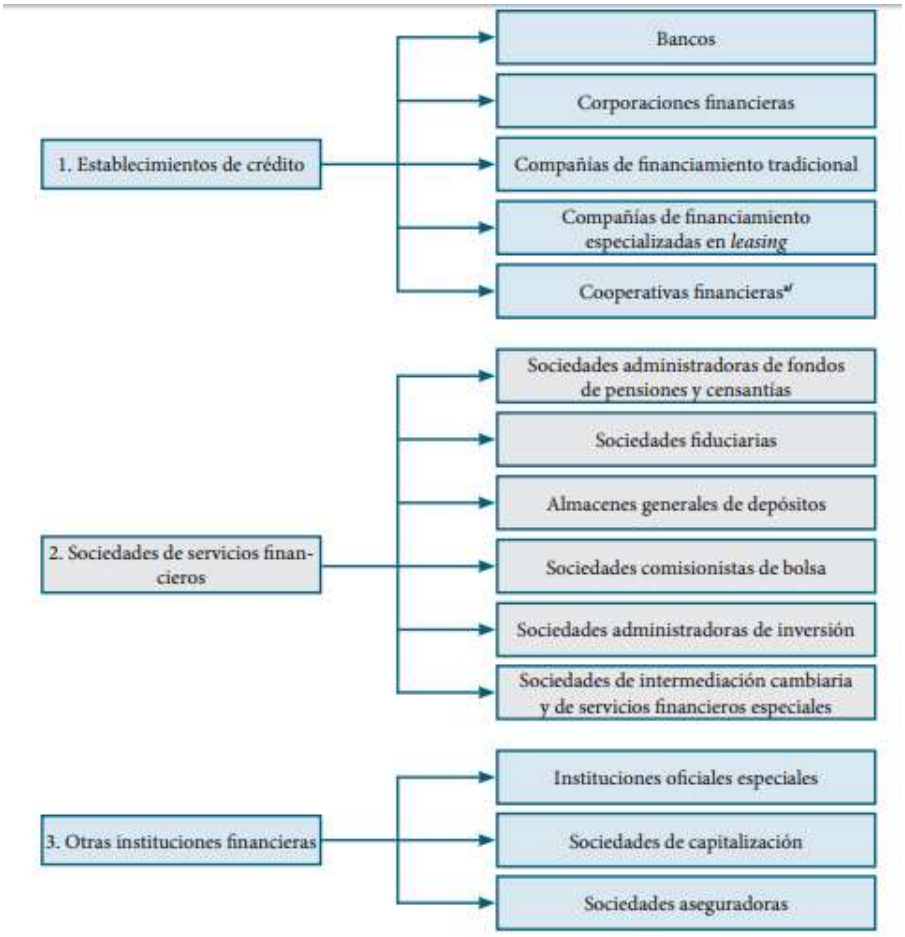
Considerando que el tema de este estudio está centrado en el Sector Bancario, es necesario abordar el contexto de todo el sistema financiero colombiano, el cual:

> Está conformado por los establecimientos de crédito (EC), las entidades de servicios financieros (ESF) y otras entidades financieras, las cuales, en su mayoría, se han agrupado mediante la figura de los conglomerados financieros, haciendo presencia tanto en el ámbito interno como externo. Luego de la crisis financiera de finales de la década de los noventa, este sector se ha venido fortaleciendo gracias, entre otras cosas, a la regulación del gobierno nacional y de la Superintendencia Financiera de Colombia (SFC), lo que se ha reflejado buenos indicadores de rentabilidad, riesgo y solvencia (…) El sector financiero colombiano está conformado por las instituciones financieras y sus fondos administrados. Bajo la vigilancia de la Superintendencia Financiera se encuentran las siguientes clases de instituciones: Los

22 Ibid, p. 1
23 Ibid, p. 1

establecimientos de crédito (EC), Las sociedades de servicios financieros (SSF) y, Otras instituciones financieras[24].

Figura 1. Sistema financiero colombiano



a/ Las cooperativas financieras son supervisadas por la SFC, mientras que las cooperativas de ahorro y crédito, y las multiactivas son supervisadas por la Superintendencia de la Economía Solidaria. El seguro de depósitos de las entidades mencionadas está a cargo del Fondo de Garantías de Entidades Cooperativas (Fogacoop).
Fuente: Estatuto Orgánico del Sistema Financiero (EOSF).

Más adelante encontramos que:

La principal función de los establecimientos de crédito es la de canalizar recursos de los agentes superavitarios de la economía hacia los deficitarios, mediante la captación de fondos del público en moneda legal, para su posterior colocación por

[24] BANCO DE LA REPÚBLICA. El Sistema Financiero Colombiano: Estructura y evolución reciente. En: Revista del Banco de la República. 2013. Vol. LXXXVI, no. 1023, p. 1.

medio de préstamos y otras operaciones activas. Después de la crisis de finales de los años noventa, y dadas las liquidaciones y fusiones de varios EC, su número se ha reducido (de 105 entidades en 1998 a 56 en diciembre de 2012) y su concentración ha venido aumentando, en tanto que el valor total de sus activos como proporción del producto interno bruto (PIB) se ha mantenido alrededor del 56% (ver tabla 1). Además de los EC, el sistema financiero está conformado por las sociedades de servicios financieros (SSF), las cuales son consideradas instituciones financieras, que si bien prestan todo tipo de servicios de tal naturaleza, no cumplen con la labor tradicional de intermediación de recursos[25].

Tabla 1. Indicadores del sistema financiero colombiano

Intermediario	Número de entidades			Activos/PIB		
	dic-98	dic-08	dic-12	dic-98	dic-08	dic-12
Establecimientos de crédito (EC)						
Bancos [1/]	38	18	23	44,5%	38,8%	50,8%
Corporaciones financieras	16	3	5	6,4%	0,8%	1,7%
Compañías de financiamiento tradicionales	27	17	16	2,0%	1,9%	1,0%
Compañías de financiamiento especializadas en *leasing*	23	10	5	1,6%	2,9%	2,2%
Cooperativas financieras	1	8	7	2,0%	0,6%	0,4%
Subtotal EC	**105**	**56**	**56**	**56,5%**	**45,0%**	**56,1%**
Sociedades servicios financieros (SSF)						
Sociedades administradoras de fondos de pensiones y cesantías	9	6	5	0,1%	0,3%	0,5%
Fondos				3,5%	14,6%	22,1%
Fiduciarias	43	26	27	0,2%	0,3%	0,3%
Fondos [2/]				1,3%	25,1%	37,1%
Comisionistas de Bolsa	56	35	26	0,2%	0,6%	0,5%
Fondos [3/]				0,2%	0,6%	1,3%
Subtotal SSF	**108**	**67**	**58**	**0,5%**	**41,5%**	**61,7%**
Total EC y SSF	**213**	**123**	**114**	**57,1%**	**86,5%**	**117,8%**

Fuente: Comunicado de prensa de la SFC y cálculos del Banco de la República.
1/ Para diciembre de 1998 incluye los bancos especializados en crédito hipotecario. Para las demás fechas éstos forman parte de los bancos comerciales.
2/ Corresponde a la administración de los fondos de inversión colectiva (antes carteras colectivas), pensiones voluntarias, pasivos pensionales y otros activos fideicomitidos. A diciembre de 1998 sólo incluye los fondos de inversión colectiva, única información disponible para esa fecha.
3/ Corresponde a la administración de los fondos de inversión colectiva, única información disponible.

Finalmente:

25 Ibid, p. 15

En particular, el papel de este grupo de entidades es el de prestar asesoría financiera especializada en la administración de recursos. Desde el punto de vista normativo a este grupo pertenecen instituciones como las sociedades fiduciarias, los almacenes generales de depósito, las sociedades administradoras de fondos de pensiones y cesantías, y las sociedades de intermediación cambiaria y de servicios financieros especiales; sin embargo, para efectos de agrupar aquellas entidades que administran no solo recursos propios, sino también de terceros, se pueden adicionar las sociedades comisionistas de bolsa (SCB) y las sociedades administradoras de inversión (SAI). Los riesgos que se generan en la actividad de las SSF difieren de los que se originan en la labor de intermediación de los EC, dado que las primeras su labor es de medio y no de resultado. Riesgos como el operacional, el legal y el de reputación se hacen críticos en la segunda clase de entidades, dado que la mayoría se orientan a administrar recursos[26].

2.4 MARCO LEGAL

El marco legal para esta investigación incluye referentes internacionales y nacionales, a saber:

En el contexto internacional se tuvo en cuenta a las Naciones Unidas, Resoluciones de la Asamblea General 52/91, de 12 de diciembre de 1997, 53/110, de 9 de diciembre de 1998 y 54/125, de 17 de diciembre de 1999, donde se contempla la preocupación internacional por delincuencia informática y la necesidad de combatirla. También se tuvo en cuenta Unión Internacional de Telecomunicaciones UIT quien propuso en 2007 una agenda sobre seguridad informática global.

Para el caso colombiano, la Constitución Política, artículo 15 de la Carta, en lo concerniente a la intimidad de las personas y el artículo 20 relativo al derecho de información. Dentro del campo de la legislación colombiana en materia del delito informático, se encuentra la Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la Ley de Delitos Informáticos. También, dentro del marco jurídico hace parte el Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones

26 Ibid, p. 2.

3. METODOLOGÍA

El presente trabajo se enmarca dentro de un tipo de investigación descriptiva, considerando el nivel de profundidad con que se aborda el proceso investigativo. La investigación descriptiva, es un acercamiento al problema mediante el análisis argumentativo basado en el conocimiento previo que tiene el investigador, indagando sobre el estado del arte de investigaciones sobre el particular, realizados por otras personas en otros contextos y disponibles en bases de datos y fuentes secundarias

En cuanto a diseño de investigación monográfica y atendiendo un esquema de averiguación que hace referencia a la forma como se produjo un nuevo conocimiento sobre el proyecto investigativo mediante un proceso riguroso de adquisición, organización, sistematización y divulgación (teórica y reflexiva) del conocimiento, partiendo de lo simple a lo complejo, de las causas a los efectos, de las partes al todo, de los principios a las consecuencias, de allí los procesos inductivos, de lo particular a lo general y procesos deductivos, de lo general a lo particular, serán los empleados para esta investigación.

Por la naturaleza de la investigación planteada, esta tuvo un proceso de revisión, análisis y síntesis documental de base de datos de organismos internacionales, así como el análisis del marco sobre aspectos técnicos y marco jurídico en torno al delito informático o ciberdelito a nivel financiero, tanto a nivel nacional como internacional.

Las fuentes que se compilaron y analizaron son de tipo secundario, por lo tanto, implicó procesos de exploración de artículos, investigaciones que se han realizado en las principales bases de datos a nivel científico, tales como PROQUEST, ESBCO, Redalyc, Scielo, entre otras y publicaciones de organismos oficiales y entidades del sistema financiero colombiano, relacionadas con el delito financiero y marco jurídico a nivel de Colombia y también de otros contextos, especialmente de organismos internacionales que han sentado las bases para la tipificación y penalización del ciberdelito financiero en el mundo.

4. RESULTADOS

Los resultados de esta investigación son presentados en respuesta a cada uno de los objetivos planteados, por lo tanto, el orden e importancia de los temas abordados corresponde a su alcance e información analítica soportada con base en las diferentes fuentes marco de esta investigación.

4.1 EL CIBERDELITO EN EL CONTEXTO DE LA SOCIEDAD GLOBAL

El fenómeno de la globalización en los ámbitos económico, político, social, cultural y medioambiental de la sociedad, junto con el avance de las tecnologías de la información y la comunicación, han creado el llamado ciberespacio como un proceso de masificación de acceso a la tecnología, la información y la comunicación, generando grandes progresos para la humanidad, pero a la vez también han generado grandes amenazas y riesgos para la sociedad, debido a los diferentes ciberdelitos cometidos por la ciberdelincuencia que atentan contra la seguridad de las naciones, las empresas y los individuos, lo cual ha conllevado a los gobiernos, las instituciones y organismos internacionales, a plantear la necesidad de hacer un frente común para contrarrestar y generar barreras tecnológicas, jurídicas y sociales contra los delitos informáticos en cualquiera de sus modalidades y afectaciones.

Las consideraciones anteriores, permiten abordar la caracterización del ciberdelito como consecuencia del avance de las tecnologías de información y la comunicación, especialmente la influencia que ha tenido el Internet en la sociedad de la información, pero también el marco jurídico desde otros contextos, relacionados con la necesidad de implementar acciones conjuntas entre países y la comunidad internacional para combatir este flagelo, el cual está afectando a las personas, las organizaciones y los Estados del mundo globalizado.

Junto con la globalización, el ciberespacio y el Internet han traído paralelamente nuevas formas delictivas convirtiéndose en una problemática de corte transnacional, obligando a los países a la adopción de medidas globales para combatir este singular fenómeno para la comunidad internacional, los gobiernos, países, organizaciones y sociedad civil en general[27].

La afectación de los delitos cibernéticos no sólo es para países desarrollados, sino también a países emergentes y en vías de desarrollo. “Los delitos cometidos a través del Internet y redes informáticas, son de tal volumen y tan sofisticados que ha sido casi imposible cuantificar los impactos económicos, financieros y no

[27] DÍAZ GÓMEZ. Op. Cit.

financieros, especialmente el relacionado con la transferencia no consentida de activos, haciendo de los países muy vulnerables con alto riesgo frente a la ciberseguridad"[28].

Frente a la proliferación del delito informático, el reto para los países dentro de su marco jurídico, especialmente para el Derecho Penal Moderno, no se reduce a la persecución y sanción de las formas tradicionales delictuales, sino que va más allá de la lesión a bienes jurídicos, dada la necesidad de combinar criterios dogmáticos de imputación de responsabilidad, medidas de política criminal, mecanismos procesales y técnicas de investigación, que brinden garantías pero que también sean efectivas frente al complejo mundo del delito informático, la criminalidad organizada la cual ha generado sofisticadas modalidades de ataque a bienes jurídicos, como el caso de la transferencia no consentida de activos[29].

Por otro lado, el Internet y los avances de las tecnologías de la información y la comunicación en todos los ámbitos del quehacer humano, son situaciones propicias para la comisión de diferentes modalidades delictivas, lo cual hace más complejo la determinación de la auditoría y en lugar de comisión del delito, dado que éste traspasa fronteras y por lo tanto la competencia para juzgar y determinar la responsabilidad jurídico-penal de quienes intervienen y así poder esclarecer igualmente la responsabilidad de los intermediarios de servicios o proveedores de Internet se vuelve muy compleja[30].

Análogamente, el crecimiento del uso del Internet para todas las transacciones no sólo económicas, sino sociales, hace necesario ahondar más en el estudio formal del derecho en relación con las variadas aplicaciones del uso del Internet y las redes sociales, exigiendo la consolidación del Derecho de la informática que permite regular contratos vía Internet, contratos electrónicos, regulación para la privacidad y protección a las redes y bases de datos, la tipificación de delitos electrónicos, la regulación del Internet, el valor de prueba de documentos electromagnéticos, la protección jurídica de programas de cómputo, el flujo de datos por Internet, la firma electrónica y en general el comercio electrónico[31]

---

[28] ANTONESCU Mihail y BIRĂU, Ramona. Emerging Markets Queries in Finance and Business. Financial and Non-financial Implications of Cybercrimes in Emerging Countries. En: Procedia Economics and Finance. 2015; no. 32, p. 618-621.

[29] DE LUARCA, M y SAAVEDRA, J. Delitos contra el patrimonio: La Ley; 2007.

[30] FARALDO CABANA, Patricia. Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática. En: Eguzkirole. Cuaderno del Instituto Vasco de Criminología. 2007. no. 21, p. 33-57.

[31] FLORES SALGADO Lucero. Derecho informático. México, D.F.: Grupo Editorial Patria, 2014.

Las anteriores consideraciones constituyen otro desafío para los gobiernos, los marcos jurídicos, policiales y judiciales y el derecho penal en particular, para establecer lineamientos claros y procesos que sancionen el delito informático a la luz de los últimos avances tecnológicos y las nuevas modalidades delictivas, tales como "la suplantación de identidad en el comercio electrónico programa espía «*spyware*», la búsqueda de documentación bancaria o comercial «*dumpster diving*»*, «*boxing*», «*shoulder surfing*» y obtención de los datos por medio de ataques a veces muy sofisticados, como el «*phishing*», el «*smishing*», el «web *spoofing*» o el «*pharming*», todos ellos como nuevas modalidades del cibercrimen"[32].

En este sentido, los desafíos del derecho penal son enormes, por cuanto la jurisprudencia y el marco jurídico de los Estados va a la saga de las nuevas modalidades delictivas, especialmente con respecto al fraude informático, la estafa y toda la variedad de tipologías del cibercrimen organizado, que utiliza la defraudación por medios informáticos y manipulación informática** "para transferir los activos patrimoniales de personas y organizaciones, implicando la necesidad de establecer claridad frente a esta tipología de delitos en cuanto a su denominación: estafa telemática, estafa por computación, fraude informático"[33].

El delito informático colombiano mediante la utilización de software, permite la trasferencia de fondos, cancelación de deuda o reconocimiento de crédito, manifiesto en tres formas: introducción de datos falsos, manipulación de datos y salida de resultados con beneficios económicos. Bajo esta modalidad está la transferencia no consentida de activos patrimoniales, donde interviene una máquina manipulada por un delincuente con el fin de afectar los bienes muebles como bienes inmuebles, denominación los activos patrimoniales[34]

---

[32] FARALDO CABANA. Op. Cit, p. 10.

[33] GARCÍA GARCÍA-CERVIGÓN, Josefina. El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. En: Icade Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales. 2008, no. 74, p. 299.

[34] Ibid. p. 300

* Estos programas pueden usarse para reunir información confidencial contenida en un ordenador sin que el usuario lo perciba. No son difíciles de encontrar, puesto que se utilizan también con fines lícitos: por ej., para que el empresario pueda controlar el ordenador del trabajador o los padres el del hijo.

** La manipulación informática se define como "toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deban ser tratados automáticamente o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial". Ibid, p. 306

En otras palabras, el ciberespacio y la utilización del Internet han abierto camino a una multiplicidad de delitos informáticos, un desafío permanente para el derecho penal puesto que los bienes jurídicos de patrimonio u orden socioeconómico, se encuentran ante nuevos riesgos y el derecho penal debe dar respuesta de manera acertada y bajo principios de colaboración internacional, dada la complejidad para su detección y aplicación de la justicia. El derecho penal debe ajustarse a un nuevo ordenamiento de la realidad delictiva para proteger los bienes jurídico-penales bajo el imperativo del respeto al principio de legalidad penal ante nuevas formas delincuenciales[35]

Como se comentó anteriormente, crece la vulnerabilidad frente a terceros en los sistemas informáticos, la interceptación de mensajes y definitivo en nuevos ámbitos de indefensión de los ciudadanos con respecto a la criminalidad organizada nacional e internacional, la cual tiene como dogma la destrucción de todo vestigio probatorio, generando con ello la impunidad ante nuevos escenarios delincuenciales[36].

Dicho de otro modo, el crecimiento permanente de la criminalidad informática en todos los ámbitos que implica la utilización de redes informáticas, motivó para que en el año 2001 se realizara la Convención de Budapest, como una respuesta de la sociedad internacional para dotar de un instrumento de lucha contra el cibercrimen organizado en sus modalidades más manifiestas: infracciones contra la confidencialidad; infracciones y fraude informático; lucha contra la pornografía infantil y delitos contra la propiedad intelectual y conexos[37]

En este sentido:

> La nueva sociedad del conocimiento, la información y la comunicación cada vez cobra mayor vigencia el llamado Derecho Informático para poder hacer frente a la delincuencia organizada, el cual incluye un conjunto de normas jurídicas para regular la utilización de los bienes y servicios informáticos en la sociedad, régimen jurídico de software, derecho de redes de transmisión de datos, documentos electrónicos, contratos electrónicos, régimen jurídico de las bases de datos, derecho

---

35 GARCÍA NOGUERA, Isabel. La reforma penal de la falsificación, tráfico y uso ilícito de tarjetas bancarias. En: IDP: revista de Internet, derecho y política. 2007. No. 5, p. 101.

36 GIMENEZ GARCÍA. Joaquín. Delito e informática: algunos aspectos de derecho penal material. En: Eguzkilore: Cuaderno del Instituto Vasco de Criminología. 2006, no. 20, p. 197-215.

37 DE LA MATA BARRANCO, Norberto y HERNANDEZ DIAZ, Leyre. Los delitos vinculados a la informática en el Derecho penal español. En: Derecho penal informático. 2010, p. 159-200.

> de la privacidad, delitos informáticos y otras conductas nacidas del uso de ordenadores y de redes de transmisión de datos[38].

Como se planteó anteriormente, la globalización y las transformaciones económicas que la explican han hecho posible la aparición, desarrollo y masificación de las nuevas tecnologías de la información. Paralelamente, el desarrollo tecnológico ha traído de la mano nuevas formas delictuales que tienen por medio o finalidad los sistemas informáticos e Internet. “Las peculiaridades de estos nuevos tipos exigen un tratamiento conjunto y coherente, y del mismo modo, su problemática particular involucra elementos transnacionales, lo que obliga a la utilización de la cooperación internacional para la adopción de medidas globales”[39].

Ahora bien, los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo[40].

Dada la proliferación de los delitos informáticos en el mundo, ha dado lugar a varias iniciativas de normativas a nivel internacional sobre delincuencia informática, las cuales datan de finales de los años 70 y surgen en el seno del Consejo de Europa. De la Conferencia auspiciada por el Consejo de Europa en 1976 sobre aspectos criminológicos de la delincuencia económica celebrada en Estrasburgo nace la primera clasificación de delitos informáticos, centrados fundamentalmente en el uso indebido de ordenadores y de programas informáticos[41]. Ya en la década de los 80 comienza a trabajar en el Consejo de Europa una comisión de expertos dedicados al análisis de las cuestiones jurídicas relacionadas con la delincuencia informática, cuyo trabajo constituye la base de la primera recomendación del Comité de Ministros del Consejo de Europa sobre delitos informáticos[42].

Los constantes desafíos que enfrenta la sociedad y los Estados, ocasiona la

> necesidad de buscar la cooperación internacional para una armonización del Derecho sustantivo, así como en el ámbito procesal, que redunde definitivamente en

---

38 HERNÁNDEZ DÍAZ, Leyre. El delito informático. En: Eguzkilore: Cuaderno del Instituto Vasco de Criminología. 2009, no. 23, p. 227-243.

39 FLORES. Op. Cit.

40 GANDINI. Op. Cit.

41 GÓMEZ VIEITES, Álvaro. Auditoría de seguridad informática. Madrid: RA-MA Editorial, 2014.

42 FLORES. Op. Cit., p.3

> un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales. Para lograrlo, la cooperación internacional, que se materializa principalmente a través de convenios internacionales, deberá reunir unos requisitos mínimos cualitativos. El Convenio sobre la Cibercriminalidad del Consejo de Europa se presenta como una solución internacional existente para el tratamiento de la cuestión ciberdelictual. A pesar de sus deficiencias, se convierte en una adecuada herramienta para la armonización legislativa interestatal y la lucha contra el ciberdelito[43].

Las Naciones Unidas también han tomado partido en este campo, se destacan, por una parte, instrumentos normativos genéricos producidos dentro de los trabajos de la Asamblea General. En el origen de la preocupación de Naciones Unidas por la delincuencia informática deben citarse las Resoluciones de la Asamblea General 52/91, de 12 de diciembre de 1997, 53/110, de 9 de diciembre de 1998 y 54/125, de 17 de diciembre de 1999, orientadas las tres a promocionar la organización de cursos prácticos de carácter técnico sobre análisis y prevención de la delincuencia informática, todo ello dentro de la actividad de los Congresos de Naciones Unidas sobre la Prevención del Delito y Tratamiento del Delincuente [44].

De otro lado, en las dos cumbres mundiales sobre sociedad de las informaciones celebradas, respectivamente, en Ginebra (2003) y Túnez (2005), la Asamblea General de Naciones Unidas encomendó a la Unión Internacional de Telecomunicaciones UIT la tarea de coordinar los trabajos sobre ciberseguridad global. Fruto de este mandato, la UIT propuso en 2007 una agenda sobre seguridad informática global con siete objetivos estratégicos básicos, uno de los cuales consistía en la elaboración de propuestas normativas de bases o de modelos aplicables a la ciberdelincuencia a nivel mundial[45].

Frente a la globalización y el ciberespacio donde también se puede decir que se dan los fenómenos de masificación de la tecnología, la información y las comunicaciones, lo cual ha permitido el desarrollo y el progreso de la humanidad, son aspectos eminentemente positivos que merecen destacarse en el contexto de la sociedad de la información y la comunicación, pero también está el aspecto negativo, que junto al progreso y la globalización también prolifera la ciberdelincuencia, lo cual ha llevado a las organizaciones y algunos gobiernos del mundo a tomar mayor conciencia de la perspectiva de futuro y la subyacente amenaza, para actuar mancomunadamente y construir barreras no sólo tecnológicas, sino también jurídicas y sociales que permitan enfrentar con probabilidades de éxito ese gran mapa de riesgos generado por los delitos informáticos. Como consecuencia, se han diseñado, divulgados y aplicados no sólo modelos, sistemas, herramientas y procedimientos de seguridad informática, sino también el necesario complemento legal para combatir el delito, además de la

---

43 GÓMEZ. Op. Cit.

44 MIRO LLINARES. Op. Cit.

45 FLORES. Op. Cit, p. 6

capacitación y preparación especializada para manejar estos componentes de seguridad, de manera integrada y cada vez más generalizada entre la sociedad[46].

El ciberdelito constituye hoy en día un desafío permanente para la comunidad internacional. En este contexto uno de los países más desarrollados como lo es Estados Unidos, ha iniciado un proceso de concientizar a la comunidad internacional, a los diferentes países para que, a través del Derecho y el marco jurídico de cada uno, intente enfrentar no sólo a nivel interno sino a nivel global la posibilidad de frenar y castigar la comisión de delitos que afecte la relación de las personas, las organizaciones y la sociedad en general. Hay necesidad, por tanto, de regular el uso del ciberespacio con normas no sólo técnicas, ni tampoco únicamente con códigos de conducta voluntarios, sino con normas jurídicas eficaces y vinculantes que garanticen los principios y valores de los modernos ordenamientos jurídicos. También la necesidad de superar la dificultad de regular el ciberespacio, más en concreto, de tipificar penalmente las conductas que deben ser sancionadas en el ciberespacio[47].

Los nuevos retos y nuevos problemas que conlleva la existencia del ciberespacio y el Internet como medio de comunicación ha originado lo que ha sido conocido como «ciberdelincuencia». Por su singularidad con respecto a la delincuencia tradicional, “este fenómeno exige una consideración especial por parte del Derecho Penal, puesto que la mayor parte de los métodos clásicos, no son los más adecuados por cuanto la diversidad de delitos cometidos en el ciberespacio, muchas veces rebasan la jurisdicción del respectivo Estado y por lo tanto hay necesidad de recurrir a la conformación de verdaderas redes inter estatales para la persecución y castigo”[48].

Finalizamos este análisis de los antecedentes del ciberdelito en una sociedad global, sus características, los avances en términos legislativos y tratamiento por parte de la comunidad internacional como un flagelo que azota a la sociedad, dada su complejidad y expansión por fuera de las fronteras de la territorialidad nacional. A continuación, se analiza el ciberdelito en Colombia y su tratamiento delictivo a la luz de la legislación vigente, haciendo énfasis en el delito financiero, tema central de esta investigación.

4.2 EL CIBERDELITO EN COLOMBIA Y SU TRATAMIENTO JURÍDICO LEGAL

La clasificación de los principales delitos informáticos en Colombia como una aproximación a la caracterización y definición, dado el auge en los últimos años

---

46 PALAZZI, Pablo A. Los delitos informáticos en el Código Penal. Buenos Aires: Abeledo-Perrot, 2009, p. 130.

47 FLORES. Op. Cit.

48 DIAZ GÓMEZ. Op. Cit., p. 182.

como consecuencia del desarrollo de las tecnologías de la información y la comunicación, especialmente el uso del Internet, dado que Colombia es uno de los países de la subregión con mayor conectividad y crecimiento en su uso. Podemos clasificar los principales delitos informáticos en cuatro grupos: - Confidencialidad – Integridad – Disponibilidad de los datos – sistemas informáticos.

En este sentido, los delitos informáticos que se identifican en Colombia están relacionados con aquellos que afectan el patrimonio económico, aquellos que buscan el abuso de menores, los que afectan a la propiedad intelectual y aquellos que afectan la información como bien jurídico. Al respecto Manjarrés & Jimenez Tarriba realiza una clasificación detallada sobre las diferentes modalidades de delitos que se cometen en el país, las cuales:

- Afectan el patrimonio económico: banca virtual, phishing, key logers, falsas páginas, venta a través de portales de compra y venta, falsos premios.
- Buscan el abuso de menores: comercializan videos, fotografía, audio, texto, falsas agencias, salas de chat.
- Afectan la propiedad intelectual: descargas de programas y comercialización de obras sin pagar derechos de autor.
- Afectan la información como bien jurídico: como por ejemplo cuando algunos empleados usan sus privilegios o permisos para acceder a información que es secreto de la empresa y luego entregarla a la competencia, teniendo como base el desarrollo que han tenido.

Dentro de la gama de delitos descrito anteriormente, está relacionado fundamentalmente con la transferencia no consentida de activos y por lo tanto corresponde al Estado la protección penal del patrimonio frente a las diferentes modalidades del ciberfraude, el cual es cometido mediante la planificación previa a través del envío de spam de phishing, la infección de spyware y malware para el posterior ataque patrimonial, un delito de resultado que se consume con el perjuicio patrimonial producido por la transferencia no autorizada de activos patrimoniales[49].

Como se analizó en el aparte anterior, la globalización ha traído consigo el uso masivo de la tecnología en todos los ámbitos, especialmente importante, tanto para el ciudadano como para el comercio, es el uso de la banca a través de la red, no obstante, ello también ha conllevado que crezca el ciberdelito a fin de desviar los dineros de los cuentahabientes. A este respecto se menciona que el 98,5 % de los riesgos bancarios en América Latina y el Caribe son digitales o informáticos, según un estudio de la Federación Latinoamericana de Bancos –FELABAN - presentado en Panamá[50].

---

49 MIRÓ LLINARES F. Op. Cit., p. 8

50 JAVATO MARTÍN, María. Las tarjetas de crédito y débito: aspectos penales. En: Cuadernos de la Cátedra de Seguridad Salmantina. 2013, no.10, p.12.

Para el caso colombiano dentro del contexto de los países de la subregión, los avances significativos en términos de conectividad y utilización del Internet y las TIC, son muy significativas en el crecimiento de la utilización de redes sociales, el comercio electrónico y las diversas transacciones en línea, especialmente en el campo financiero. Esto ha originado, que también los delitos informáticos hayan proliferado en todas sus manifestaciones y tipificaciones, por lo tanto, le compete al Estado y las autoridades, legislar y sentar las bases para la persecución de actividades delictivas y castigar ejemplarmente a los infractores[51]. Sin embargo, en la práctica el ciberdelito, especialmente la transferencia no consentida de activos para el caso colombiano, goza de mucha impunidad.

Dentro de la gama de delitos informáticos que se cometen en el país, llama la atención la denominada estafa o movilidad de activos sin consentimiento*, especialmente cuando se refiere a la afectación de las transacciones financieras a través de las diferentes entidades de intermediación. Si bien en Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del 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 tecnologías de la información y las comunicaciones, entre otras disposiciones", aún existen vacíos jurídicos desde el punto de vista del Código Penal, que se hace necesario analizar y profundizar para lograr incorporar su modernización acorde a las nuevas modalidades del ciberdelito[52].

El Código Penal colombiano prevé en el artículo 269J las figuras típicas de Transferencia no consentida de activos y tenencia de software destinado al fraude, propias de los delitos informáticos en sentido estricto que, además de la seguridad

---

[51] GONZÁLEZ RUS, Juan José. Delitos contra el patrimonio y contra el orden socioeconómico (V). Las defraudaciones. La estafa. En: Sistema de Derecho Penal Español, Parte Especial. Madrid: Dykinson, 2011, p. 481-511.

[52] SALAZAR, Juan F. Situación normativa de la Sociedad de la Información en Colombia. En: Criterio Jurídico. 2011. vol. 9, no. 1, p. 89-103.

* Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa (Código Penal).

de la información informatizada, protegen el patrimonio económico. La presente investigación busca realizar un estudio breve en relación con el concepto de "ciberdelito", el bien jurídico protegido por la norma citada y los elementos objetivos y subjetivos que estructuran este tipo de incriminaciones jurídicas que, en el medio, constituyen un avance imprescindible para completar el "microsistema" de seguridad de la información y los datos en el Código penal vigente[53].

El informe de la FELABAN fue presentado durante el XXX Congreso Latinoamericano de Seguridad Bancaria, que se celebró en la capital panameña. Los bancos de América Latina enfrentan tres riesgos informáticos principales:

- La clonación de tarjetas,
- La suplantación de identidad en compras no presenciales y
- El *Phishing*

Este último término se utiliza para describir un modelo de abuso informático en el que un ciberdelincuente se hace pasar por una persona o una institución de confianza para obtener información confidencial del cliente de forma fraudulenta, por lo tanto, la incorporación de estrategias para minimizar riesgos como la tecnología chip en las tarjetas débito y crédito y el uso en las compras *online* de "*token de seguridad*", un dispositivo electrónico que usan los clientes para validarse, son entre otros algunos de los avances de la industria financiera para combatir el ciberdelito[54].

En Colombia a medida que los usuarios del sistema financiero han venido accediendo con más facilidad durante los últimos años a medios digitales (como teléfonos inteligentes, tabletas y ordenadores personales) para realizar transacciones en línea, las posibilidades para que los delincuentes cometan fraudes en línea en Colombia parecen tornarse cada vez más fuertes. Esta es una de las advertencias que lanzó ASOBANCARIA (el gremio de la banca) el cual señaló –con cifras de la Fiscalía General de la Nación como soporte– que las denuncias por ciberdelincuencia aumentaron.

---

[53] POSADA MAYA, Ricardo. El delito de transferencia no consentida de activos [en línea]. En: Revista de Derecho, comunicaciones y Nuevas Tecnologías. 2012 [revisado 1 de marzo de 2016], no. 8, p. 4-27. Disponible en internet: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics120.pdf

[54] QUINTERO CHAPARRO Sandra R y SUÁREZ LEÓN Sandra P. Comisión de conductas punibles en el internet en Colombia. Bogotá: Universidad Militar Nueva Granada, 2012.

.

La tasa de delitos informáticos en el país viene creciendo más rápido que lo visto en fenómenos como el narcotráfico y los homicidios. Es necesario replantear la concepción que se tiene del derecho penal para poder entender este fenómeno para enjuiciar a personas de bandas dedicadas a delitos informáticos[55].

Una buena parte de los fraudes que se dan en el sistema financiero colombiano, explica Gina Pardo, directora de gestión operativa y de seguridad de ASOBANCARIA, no se presenta a través de mecanismos sofisticados sino de correos y aplicaciones móviles. A pesar de que se usan métodos que en apariencia no son complejos, dado que detrás de los delitos informáticos en el país se esconden estructuras delincuenciales organizadas a las que las autoridades deben perseguir y enjuiciar[56].

Tal como se describe, los ataques de *phishing* contra entidades financieras constituyen una de las principales preocupaciones y ha obligado a las entidades a invertir grandes sumas de dinero anualmente en la prevención, detección y retirada de este tipo de ataques. Esta operación es tan masiva y el tiempo crítico que generalmente no hay tiempo para realizar el análisis para buscar patrones y correlaciones entre los ataques[57].

El sistema financiero colombiano está conformado por los establecimientos de crédito (EC), las entidades de servicios financieros (ESF) y otras entidades financieras, las cuales, en su mayoría, se han agrupado mediante la figura de los conglomerados financieros, haciendo presencia tanto en el ámbito interno como externo. Su constitución se da principalmente por las instituciones financieras y sus fondos administrados y bajo la vigilancia de la Superintendencia Financiera las siguientes son las clases de instituciones: Los establecimientos de crédito (EC); Las sociedades de servicios financieros (SSF) y, Otras instituciones financieras[58].

El uso de la banca en casa es importante para las instituciones financieras, dado que en ella se establecen operaciones con costes reducidos en comparación con la gestión tradicional de los bancos físicos, pero también tiene ventajas desde el punto de vista del usuario, reduciendo el tiempo de espera para el servicio y

---

55 MANJARRÉS, Iván, JIMENEZ TARRIBA, Farid. Caracterización de los delitos informáticos en Colombia [en línea]. En: Revista Pensamiento Americano. 2014 [revisado 2 de marzo de 2016]. vol. 5, no. 9, p. 79. Disponible en internet: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

56 POSADA MAYA. Op. Cit., p. 6.

57 GÓMEZ VIEITES. Op. Cit., p. 4.

58 RODRÍGUEZ ZÁRATE, Alejandro. Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos [en línea]. En: Vniversitas, 2015 [revisado 3 de marzo de 2016], no. 128. p. 285-314. Disponible en internet: http://revistas.javeriana.edu.co/index.php/vnijuri/article/view/10176/8357.

también para permitir que un servicio que se pretende que sea rápido y eficiente, en cualquier momento y en cualquier lugar[59].

Lo anterior no significa que en Colombia no hayan existido avances en términos de legislación contra el delito. Haciendo un análisis retrospectivo sobre la legislación colombiana en materia del delito informático, la Ley 1273 del 5 de enero de 2009, fue reconocida en Colombia como la Ley de Delitos Informáticos, tuvo sus propios antecedentes jurídicos. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas[60] .

La investigación realizada refleja la importancia de un tratamiento analítico de revisión pertinente a fin de generar nuevo conocimiento jurídico para el debate, el análisis y la modernización de la jurisprudencia en este campo tan amplio y tan desafiante para la sociedad y el mundo en general, especialmente en el tratamiento a la estafa o estafa financiera o transferencia no consentida de activos

Sin embargo, para el caso colombiano dentro del contexto de los países de la subregión, los avances significativos en términos de conectividad y utilización del Internet y las TIC, el crecimiento de la utilización de redes sociales, el comercio electrónico y las diversas transacciones en línea, especialmente en el campo financiero. Esto ha originado, que también los delitos informáticos hayan proliferado, especialmente en materia de transacciones financieras, tipificando lo que en el código penal se denomina *transferencia no consentida de activos* y por lo tanto, le compete al Estado y las autoridades, legislar y sentar las bases para la persecución de actividades delictivas y castigar ejemplarmente a los infractores.

La anterior afirmación se sustenta en Grisales Pérez, quien toma como referencia el reporte económico semanal–de fecha 29 de octubre de 2012-elaborado por el principal gremio de los bancos ASOBANCARIA, donde se señala las principales modalidades de delito que afecta al sector bancario, así como las pérdidas que soporta permanentemente frente a los ataques de la ciberdelincuencia, situación que amerita especial atención por parte de la justicia de las autoridades del Estado colombiano. En dicho informe se señala que:

---

59 CARRILHO NEGAS, Mario F.; MARTINHO LOPES, José M. y ROSARIO NEGAS Elsa I. Homebanking users and more relevant security risks associated. En: Iberian Conference on Information Systems and Technologies, CISTI. 2013. p. 1-6.

60 RODRÍGUEZ ARBELÁEZ. Op. Cit.

> Las tipologías de fraude que afectan al sector bancario y a sus clientes van desde el fleteo y el taquillazo hasta complejos delitos informáticos. Dentro de estos últimos se puede hacer referencia a modalidades como el *phishing* (suplantación de sitios web), instalación de troyanos o software espía para el hurto de información, el acceso abusivo a sistemas informáticos y la clonación de tarjetas débito y crédito. El uso cada vez mayor de los canales electrónicos para la realización de operaciones bancarias y los avances tecnológicos, que le facilitan al delincuente adquirir herramientas y establecer contacto con organizaciones ilegales de otros territorios, son factores que han llevado a una tendencia creciente de los ataques tecnológicos o informáticos contra los establecimientos de crédito[61].

Lo anterior, permite aseverar que dentro de la gama de delitos informáticos que se cometen en el país, llama la atención la llamada estafa o movilidad de activos sin consentimiento, especialmente cuando se refiere a la afectación de las transacciones financieras a través de las diferentes entidades de intermediación.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa (Código Penal).

Ahora bien, los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo[62].

Colombia tiene una economía global, con firma de tratados bilaterales y multilaterales con diversos países, que reclaman la necesidad de implementar a través de la colaboración entre naciones, una legislación acorde a la proliferación

---

61 GRISALES PÉREZ, Giovanni S. Análisis dogmático de las conductas de hurto por medios informáticos y semejantes (art. 269i) y transferencia no consentida de activos (art. 269j) Ley 1273 de 2009 [en línea]. Medellín: Universidad EAFIT. 2013 [revisado el 3 de marzo de 2016]. Disponible en internet: https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf?sequence=1

62 GANDINI. Op. Cit., p. 8

para realizar avances significativos como la tipificación del delito informático de transferencia no consentida de activos.

En este sentido, cabe resaltar los antecedentes legislativos del delito de hurto por medios informáticos que, en sentencia de la Corte Suprema de Justicia, señala:

> Debido a la creciente criminalidad en materia informática y a la necesidad de que Colombia alcanzara un nivel normativo similar al de otros países que, de tiempo atrás, venían sancionando infracciones relacionadas con el abuso de los sistemas informáticos y los datos personales –Convenio sobre la ciberdelincuencia de Budapest (2001), adoptado por el Consejo de Europa-, en el Congreso de la República surgió una primera iniciativa –Proyecto de Ley No. 042 de 2007 Cámara*- destinada a modificar y adicionar algunos tipos penales regulados en el capítulo VII del Código Penal relativos a la «Violación a la intimidad, reserva e interceptación de comunicaciones»[63] y a endurecer las penas del hurto calificado, el daño en bien ajeno, la violación de reserva industrial o comercial y el espionaje, cuando quiera que se ejecuten utilizando medios informáticos o se vulneren las seguridades informáticas de las víctimas.[64]

La anterior situación descrita, define uno de los problemas del campo jurídico, dar respuesta a la protección del bien jurídico y el patrimonio económico en la era de la globalización, del Internet y la banca electrónica** y banca móvil*** en un Estado Social de Derecho. “En definitiva, es innegable que hay un punitivismo ampliamente desarrollado en relación con la cibercriminalidad, pero también debemos tener en cuenta que estamos ante uno de los temas más necesitados de protección penal. Será necesario equilibrar la balanza introduciendo los principios garantistas propios del Estado Social y Democrático de Derecho”[65].

Los avances vertiginosos de las tecnologías de la información y el Internet, con ello el aumento de la cibercriminalidad, reclaman la necesidad de proteger a las personas de nuevas conductas perniciosas a través de la Red, es indudable que el

---

* Cuyo ponente fue el doctor Germán Varón Cotrino.

63 Concretamente, la posesión de instrumentos aptos para interceptar comunicaciones privadas, el acceso abusivo a un sistema informático, la violación a la disponibilidad de datos informáticos y sus circunstancias de agravación

64 Sentencia de la Corte Suprema de Justicia - Sala de casación penal nº 42724 de 11 de febrero de 2015.

** Banca electrónica: Desarrollo de productos financieros a través de canales o medios electrónicos, entre los que se encuentra la banca a través de portales de internet, cajeros electrónicos, servicios de acceso remoto a sistemas de información, banca móvil, banca telefónica entre otros. O en general a través de cualquier canal o medio electrónico.

*** Banca Móvil: Prestación de servicios financieros en los cuales el teléfono móvil es el dispositivo a través del cual se realiza la operación.

65 DÍAZ GÓMEZ. Op. Cit.

Derecho Penal está experimentando una nueva expansión. “De hecho, cualquier propuesta de solución de problemas, cualquier intento de mejora de las legislaciones, pasa inevitablemente por una ampliación de las conductas delictivas. Ésta parece ser la única alternativa a la protección de los bienes jurídicos que se vulneran en las distintas modalidades de delitos informáticos”[66].

En este mismo sentido, para el caso colombiano lo enmarca Posada Maya[67], al señalar la necesidad de referirse al bien jurídico, donde la normativa vigente supera la clásica discusión, al preguntarse todavía si la cibercriminalidad lesiona o pone en peligro un interés autónomo (el espacio informático como bien jurídico intermedio), o si lesiona o pone en peligro distintos bienes jurídicos tutelados, que comprenden intereses diversos de naturaleza colectiva o derechos personalísimos y personales (como el patrimonio económico) o ambos, que incluyen la seguridad de la información y las funciones informáticas.

4.3 DESAFÍOS TÉCNICOS Y JURIDICOS FRENTE AL CIBERDELITO EN EL SECTOR BANCARIO COLOMBIANO

En este aparte, se abordan los principales aspectos relacionados con los protocolos de seguridad desde el punto de vista técnico, los cuales deben desarrollarse de acuerdo a los avances tecnológicos en materia de seguridad informática, sólo así es posible garantizar que el ciberdelito, especialmente el relacionado con los delitos financieros de la banca colombiana sean tratados con veracidad y seguridad.

Actualmente, se dispone de manera general prototipos de Seguridad de última generación, los cuales tienen como objetivo permitir que dos o más agentes puedan establecer una comunicación de manera segura en una red a pesar de ambientes hostiles, tales como Internet. El diseño de estos prototipos es particularmente propenso a errores, por eso, es difícil anticipar lo que un intruso puede lograr cuando, pretendiendo ser un participante honesto, logra interactuar dentro del sistema. Así, la verificación de protocolos de seguridad ha atraído un gran interés en la comunidad de los métodos formales, dando como resultado la aparición, en las dos últimas décadas, de una gran cantidad de técnicas/herramientas, además de buenas prácticas para mejorar su diseño[68].

Si bien es cierto en la actualidad se vive en un mundo en el que impera la necesidad de un constante intercambio de información vía Internet e Intranet,

---

66 Ibid, p. 2.

67 POSADA MAYA R. Op. Cit. p. 5

68 LÓPEZ PIMENTEL, Juan Carlos y MONROY, Raúl. Formal Support to Security Protocol Development: A Survey. En: *Computación y Sistemas.* 2008. no. 12. p. 89-108.

muchas veces dicha información debe ser confidencial, por lo que se debe proveer un medio que ofrezca seguridad para su transporte. Es importante señalar que cuando se menciona la palabra “seguro” no se refiere únicamente a la confidencialidad de la comunicación, sino también se hace alusión a la integridad de los datos que para muchas compañías y entornos de negocios puede ser un requisito mucho más crítico que la confidencialidad. Es por eso que surge IPSec el cual cuenta con innumerables características, así como cualidades que satisfacen las necesidades de seguridad, confidencialidad y autenticidad de la información. IPSec proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP entre otros) y aborda las carencias en cuanto a seguridad del Protocolo IP. Dichas carencias son muy graves, tal como se ha constatado en los últimos años, y afectan a la infraestructura misma de las redes IP[69].

4.3.1 El Protocolo IPSEC.

> IPSec es un estándar de gran utilidad que ofrece servicios de seguridad en redes IP de cualquier índole, él está formado por un conjunto de estándares del IETF (Internet Engineering Task Force) que conjuntamente proporcionan servicios de seguridad en la capa IP de las comunicaciones entre sistemas electrónicos, y por añadidura a todos los protocolos de niveles superiores que están basados en IP (TCP, UDP, ICMP, y otros). Hoy en día los protocolos basados en IP tienen una presencia universal en las redes telemáticas. Desde cualquier red local común hasta la propia Internet están basados en este protocolo para su funcionamiento. Uno de los problemas que enfrenta IP es la dificultad para asegurar las comunicaciones. Con “asegurar” no sólo se refiere a seguridad de acceso a sistemas (que es lo primero en que se suele pensar), sino también a establecer medios de comunicación que puedan evitar la intercepción de la información y su manipulación, así como asegurar la confidencialidad de los datos intercambiados[70].

4.3.2 Protocolos Básicos de IPSec.

Al respecto encontramos la siguiente información:

> El IPSec (Internet Protocol Security) es un protocolo de capa 3 específicamente diseñado para el protocolo IP, que brinda herramientas de seguridad a través de la autenticación de orígenes y la encriptación de las comunicaciones que se realicen mediante su uso. La principal particularidad que presenta este protocolo es el hecho de operar en una capa baja del modelo OSI, lo cual le permite ofrecer interoperabilidad con casi todos los protocolos de capas superiores. Este beneficio se debe a que al operar en una capa tan baja, los protocolos de altas capas no

---

69 CARBAJAL, Mauricio, *et al*. Introducción a la Seguridad con IP Seguro en Internet (Ipsec). En: Polibits. 2005. no. 32. p.16-21.

70 Ibid, p. 17

tienen necesidad de enterarse de que la red en donde transitan opera bajo IPSec, por ende no deben prepararse para trabajar con él[71].

Los servicios de seguridad proveídos por IPSec son:

1) Autenticación y autenticidad de origen: cada extremo de una comunicación IPSec deberá pasar inevitablemente por un proceso de autenticación, que validará su identidad ante el agente de control. Asimismo, cada paquete enviado en la comunicación será verificado para corroborar que realmente haya sido enviado desde la entidad que reclama haberlo efectuado.
2) Confidencialidad: las comunicaciones que se realicen con este protocolo pasarán por un proceso de encriptación fuerte que lo protegerá de divulgaciones.
3) Integridad: todo mensaje transmitido a través de IPSec pasará por verificaciones en destino para corroborar si fue recibido íntegramente o si hubo corrupción de datos
4) Anti-replay: cada paquete cuenta con una identificación propia que será utilizada únicamente para dicho paquete y luego será descartada. Esta técnica inhabilita el llamado *replay attack*, que consta de la captura y repetición de mensajes específicos por un agente malicioso, con fines de obtener réplicas de las respuestas de dicho mensaje desde destino[72].

IPSec está constituido por un conjunto de estándares de criptografía que lo dotan de sus especiales características. Utiliza algoritmos de clave pública como RSA, algoritmos de resumen digital (SHA1, MD5), certificados digitales X509 y algoritmos de cifrado de clave simétrica como DES, IDEA, Blowfish o AES. Todos estos elementos forman parte de IPSec como pequeñas piezas que se pueden conectar sin interferir unas en otras. Esto hace que sea posible utilizar todo tipo de algoritmos existentes en la actualidad o en el futuro. Sin embargo, y en aras de conseguir la mayor interoperabilidad posible, la implementación mínima de IPSec debe ofrecer ciertos elementos estándar que siempre se deben soportar. En concreto, siempre estarán disponibles los algoritmos MD5 y SHA-1 para cálculo de huellas digitales (Hashes) y los algoritmos DES y triple DES para cifrado simétrico con clave privada[73].

El funcionamiento de IPSec está basado en la existencia de dos componentes de suma importancia:

El protocolo de gestión de claves llamado IKE (Internet Key Exchange), que es el encargado de hacer las negociaciones de todos los parámetros necesarios de conexión y seguridad, incluyendo como su propio nombre indica, las claves utilizadas para el cifrado de datos.

---

71 KATZ, Matías David. Redes y Seguridad. México: Alfaomega Grupo Editor, 2013. ISBN 9788426719799

72 Ibid, p. 35

73 CARBAJAL, *et al*. Op. Cit., p. 19

El protocolo de seguridad. Éste protocolo tiene como función principal proteger el tráfico de datos en IP. El estándar define dos protocolos de seguridad que pueden ser utilizados con IPSec: Authentication Header (AH) y Encapsulating Security Payload (ESP)[74].

4.3.3 Modos de Funcionamiento de IPSec

Los protocolos de seguridad analizados proporcionan dos modos de funcionamiento que se pueden escoger tanto para AH como en ESP:

1. Modo transporte. Este modo de funcionamiento permite la comunicación punto a punto entre los nodos que se quieren relacionar con IPSec. Se utiliza cuando ambos extremos son capaces de utilizar directamente el protocolo IPSec.
2. Modo túnel. Este modo se utiliza cuando alguno de los dispositivos que se comunican (uno de ellos o ambos) no es el encargado de realizar las funciones de IPSec. Este es el modo de funcionamiento más habitual cuando se usan dispositivos de encaminamiento que aíslan una red privada de una pública, centralizando todo el proceso de tráfico IPSec en un único punto. De este modo, por ejemplo, los equipos internos de una red local y sus aplicaciones no tienen por qué implementar ni entender IPSec. Se comunican normalmente (sin protección alguna) con el nodo que procesa IPSec y es éste el que se encarga de realizar las funciones por todos ellos comunicándose con otro dispositivo IPSec en el otro extremo. De este modo se protegen las direcciones privadas, se centraliza la administración del protocolo de seguridad en un único punto, y se puede utilizar IPSec en sistemas que, en un principio, no estaban preparados para utilizarlo. Una de las principales aplicaciones del modo túnel es establecer de manera sencilla y barata Redes Privadas Virtuales (o VPN) a través de redes públicas. Ello permite intercomunicar entre sí, a través de Internet, redes locales o equipos aislados con las mismas garantías de seguridad que si estuviesen en una red privada, aunque usen internamente direcciones IP no válidas en la Red"[75].

4.3.4 Aplicaciones de IPSec en el Día a Día.

- *Control de acceso y autorización de comunicaciones*. Gracias a las capacidades de filtrado de IPSec se puede decidir exactamente cómo se realizan las comunicaciones a través de IP con cualquiera de los protocolos de alto nivel. Si además los protocolos son TCP o UDP es posible controlar qué se hace con el tráfico en función de las direcciones IP y los puertos de origen y destino. Se obtiene casi las mismas capacidades que las que ofrece básicamente un cortafuego (salvando las distancias).
- *Conexión segura de oficinas y creación de intranets distribuidas*. Con IPSec se puede hacer que las distintas sucursales y oficinas de una empresa trabajen a través de líneas ADSL o RDSI como si estuviesen en realidad en una misma red local física y sin necesidad de líneas dedicadas punto a punto: directamente sobre

---

74 Ibid, p. 21
75 Ibid, p.16

Internet y con total garantía. Esto significa un elevado ahorro de costos unido a una gran comodidad.

- *Relación segura con proveedores, distribuidores, socios, y otros agentes del entorno*. Para intercambio de información comercial y técnica, emisión de datos electrónicos (EDI) y comercio electrónico entre empresas.
- *Tele trabajo y acceso de viajantes y personal desplazado*. Los trabajadores que se encuentran de viaje o trabajan desde sus casas podrán acceder a la red de la empresa con total seguridad para buscar información en ciertas bases de datos, remitir pedidos e informes, consultar su correo interno o su agenda o acceder a la Web interna departamental[76].

IPSec es la seguridad del protocolo de internet, que constituye un marco de normas abiertas que proporciona protección a las comunicaciones a través del uso de servicios de seguridad criptográfica, garantizando los tres principios de la seguridad informática en las redes de datos: Confidencialidad, Integridad y Disponibilidad[77].

4.3.5 Protocolo de Internet versión 6

IPv6 es la nueva versión del protocolo de Internet. En 1995, la IETF (Internet Engineering Task Force) que desarrolla estándares para los protocolos de Internet, publicó una especificación para el IP de la siguiente generación, conocido como IPng (Internet Protocol next generation). Esta especificación se convirtió en 1996 en un estándar conocido como IPv6, el cual proporciona una serie de mejoras funcionales al IP existente conocido como IPv4, diseñado para ajustarse a las altas velocidades de las redes actuales y a la mezcla de flujo de datos, que incluyen audio y vídeo, pero detrás del desarrollo del nuevo protocolo se halla la necesidad imperante de nuevas direcciones. Los cambios de IPv6 con respecto a IPv4 se explican en el RFC 2460"[78]

4.3.6 Seguridad del protocolo de internet (IPSec)

IPSec es un conjunto de mecanismos de seguridad para proteger las comunicaciones que utilizan el protocolo de Internet, a través del uso de los servicios de seguridad criptográfica. Además, admite la autenticación a nivel de red de pares, de origen de datos, integridad de datos, confidencialidad de los datos (encriptación) y protección contra la reproducción. La implementación de IPSec se basa en las especificaciones elaboradas por la Internet Engineering Task Force (IETF)[79].

---

76 Ibid, p.19.

77 CONTRERAS, Josue Lobo y RICO BAUTISTA, Dewar Willmer. Implementación de la seguridad del protocolo de Internet versión 6 [en línea]. En: REVISTA GTI. 2012. vol. 11, no. 29. Disponible en internet: http://revistas.uis.edu.co/index.php/revistagti/article/view/2815

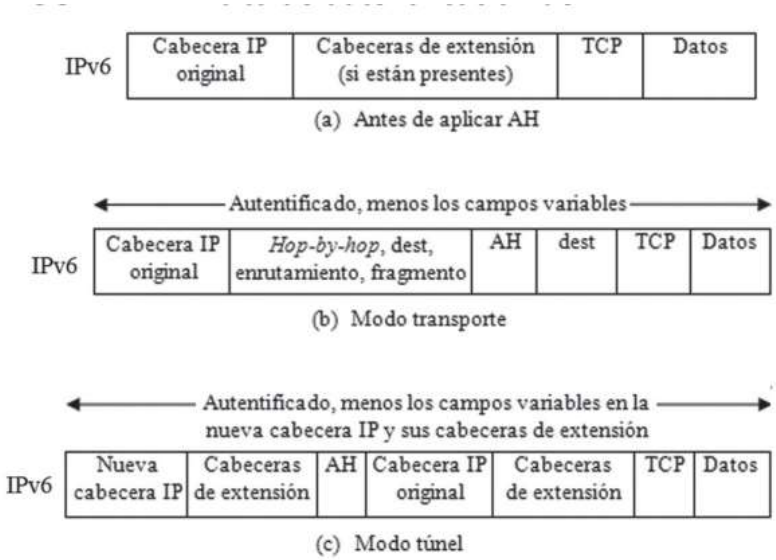
78 Ibid, p. 25

79 Ibid, p. 38

Modos de funcionamiento
Permiten dos modos de uso: modo transporte y modo túnel Tanto AH (Cabecera de autenticación) la cual proporciona autenticación e integridad a los datos trasmitidos y ESP que incluye cabecera y campos para dar soporte a la encriptación.

Modo transporte: El modo trasporte proporciona protección principalmente a los protocolos de capas superiores. Es decir, esta protección se extiende a la carga útil de un paquete IP. Algunos ejemplos incluyen un segmento TCP o UDP, que operan directamente encima de IP en la pila de protocolos de un host. Normalmente, el modo transporte se usa para la comunicación extremo a extremo entre dos hosts.

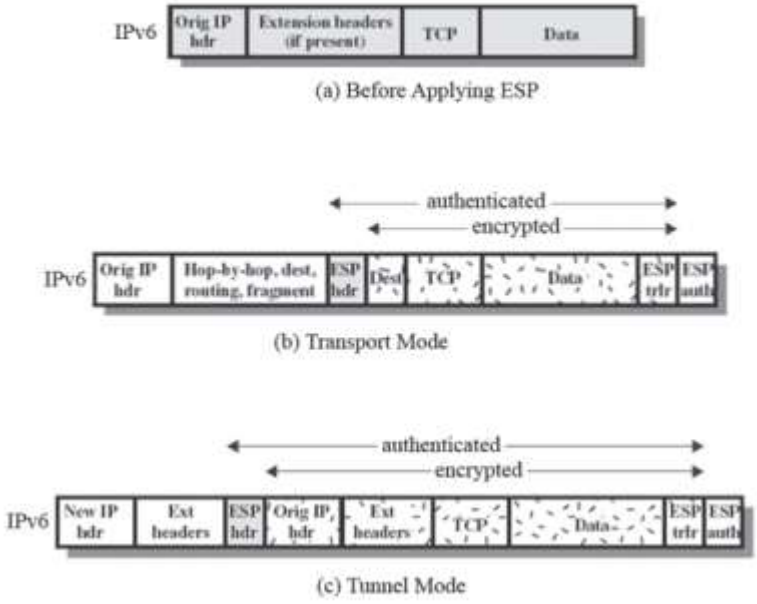
Figura 1. Ámbito de autentificación de AH.



Fuente: http://slideplayer.es/slide/2261932/

Modo túnel: El modo túnel proporciona protección al paquete IP completo. Para conseguirlo, después de que han añadido los campos AH o ESP al paquete IP, el paquete completo más los campos de seguridad se tratan como carga útil de un paquete IP «exterior» nuevo con una nueva cabecera IP exterior. El paquete original entero, o interior, viaja a través de un «túnel» desde un punto de la red IP a otro; ningún router a lo largo del camino puede examinar la cabecera IP interior. Como el paquete original esta encapsulado, el nuevo paquete, que es mayor, puede tener direcciones de origen y destino totalmente diferentes, lo cual añade seguridad. El modo túnel se usa cuando uno o los dos extremos de una SA es una pasarela de seguridad, como podría ser unos cortafuegos o un router que implementa IPSec.

Figura 2. Ámbito de cifrado y autenticación de ESP.



Fuente: http://slideplayer.es/slide/2261932/

Servicios

IPSec proporciona servicios de protección a la capa IP permitiendo que un sistema elija los protocolos de seguridad necesarios, determine los algoritmos que va a usar para los servicios y ubique las claves criptográficas necesarias para proveer los servicios solicitados.

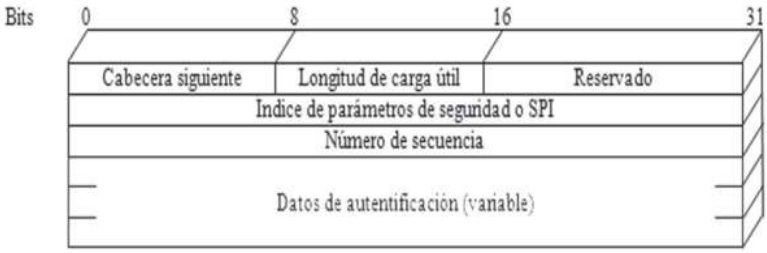
Figura 3. Servicios de IPSec

Servicio	*AH*	*ESP* (Encriptación)	*ESP* (Encriptación y Autenticación)
Control de acceso	✓	✓	✓
Integridad sin conexión	✓		✓
Autentificación del origen de datos	✓		✓
Rechazo de paquetes reenviados	✓	✓	✓
Confidencialidad		✓	✓
Confidencialidad limitada del flujo de tráfico		✓	✓

Fuente: http://flylib.com/books/en/3.190.1.135/1/

4.3.7 Protocolo de Cabecera de autenticación (AH) RFC 4302
La cabecera de autentificación proporciona soporte para la integridad de los datos y la autentificación de paquetes IP. La característica de integridad garantiza que no es posible que se produzca modificación no detectada en el contenido de un paquete durante la transmisión. La característica de autentificación permite que un sistema final o dispositivo de red autentifique al usuario o aplicación y filtre el tráfico adecuadamente; también evita los ataques de suplantación de dirección que se observan hoy en día en internet. La cabecera de autenticación se compone de seis campos, como se ilustra en la figura siguiente.

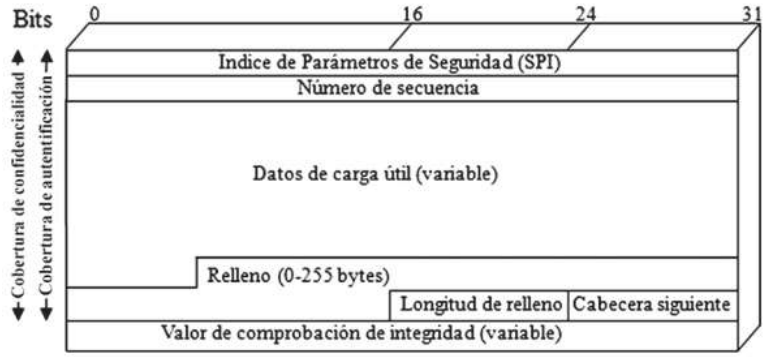
Figura 4. Cabecera de autentificación IPSec



Fuente: http://slideplayer.es/slide/2261932/

La carga de seguridad encapsuladora se compone de siete campos, como se ilustra en la figura siguiente:

Figura 5. Los siete campos de carga de seguridad encapsuladora



Fuente: http://slideplayer.es/slide/2261932/

4.3.8 Protocolo de Intercambio de claves de internet (IKE) RFC 4306
La parte de gestión de claves de IPSec implica la determinación y distribución de claves secretas. La especificación actual de la arquitectura de IPSec asigna soporte para dos tipos de gestión de claves:

Manual: Un administrador de sistema configura manualmente cada sistema con sus propias claves y con las llaves de otros sistemas que se comunican. Esto es práctico para entornos pequeños relativamente estáticos.

Automática: Un sistema automático permite la creación bajo demanda de claves para las SA y facilita el uso de claves en un sistema distribuido grande con una configuración cambiante. El protocolo de gestión automatizada de claves por defecto para IPSec se conoce como ISAKMP/Oakley y se compone de los siguientes elementos:

> *Protocolo de determinación de Claves OAKLEY*: Es un protocolo de intercambio de claves basado en el algoritmo Diffie-Hellman, pero que proporciona seguridad adicional. Oakley es genérico, ya que no dicta formatos específicos.
> *Asociación de seguridad y Protocolo de gestión de claves ISAKMP*: Proporciona un marco de trabajo para la gestión de claves de Internet y el soporte de protocolos específicos, incluyendo formatos para la negociación de los atributos de seguridad[80]

4.3.9 Otras tecnologías de seguridad

Para complementar este aparte de marco técnico, es conveniente analizar otras tecnologías existentes en materia de seguridad y protocolos, como la que se describe a continuación.

Secure Shell (SSH)

> SSH permite conectarse a otras máquinas o trasmitir ficheros de forma segura a través de Internet u otros medios no seguros. Los algoritmos de cifrado se emplean para autentificar ambos lados de la conexión, cifrar todos los datos y proteger la integridad de los mismos. Existen actualmente dos protocolos SSH: SSH1 y SSH2. El protocolo SSH2 es una completa re-implementación del protocolo SSH1, cifrando diferentes partes del paquete, empleando diferentes algoritmos de intercambio de claves, etc., de modo que es considerado más seguro, y evita algunas conocidas vulnerabilidades de las implementaciones de SSH1[81.]

El protocolo SSH se divide en tres partes principales: la negociación del algoritmo, la autentificación y el cifrado de los datos. La negociación del algoritmo es la responsable principal de determinar los algoritmos de cifrado, los algoritmos de compresión y los métodos de autentificación soportados y empleados entre el cliente y el servidor. La autentificación, además se encuentra dividida en dos

---

80 Ibid. p. 29

81 GONZÁLEZ, Iván, GÓMEZ-ARRIBAS, Francisco. J. y LÓPEZ-BUEDO, Sergio. Implementación de SSH sobre un Sistema Auto-Reconfigurable [en línea]. En: VI Jornadas de Computación Reconfigurable y Aplicaciones, JCRA 2006. Cáceres, Universidad de Cáceres Septiembre 12-14, 2006. Disponible en internet: http://hdl.handle.net/10486/667396

partes: el intercambio de claves y la autentificación del usuario. El propósito del intercambio de claves es doble. Primero, permite la autentificación del servidor por el cliente. Segundo, establece una clave compartida que es empleada como clave de sesión para el cifrado de todos los datos a transmitir entre las dos máquinas, empleando algoritmos de clave simétrica. Además, se genera un *hash* para la comprobación de la integridad de los datos[82].

Métodos de cifrado en SSH
SSH intenta proveer una fuerte seguridad, empleando métodos de criptografía, de forma transparente al usuario. SSH1 ofrece cuatro algoritmos de cifrado DES, 3DES, IDEA y Blowfish. SSH2 elimina el soporte para DES (algoritmo roto) e IDEA (problemas de patentes), y añade tres nuevos algoritmos: AES (Rinjdael), Twofish y CAST. SSH1 emplea el algoritmo de autentificación RSA, mientras que SSH2 lo ha cambiado por DSA. Estos cambios fueron realizados para eliminar los problemas de patentes, IDEA y RSA, e incrementar el nivel de seguridad en SSH2 empleando algoritmos más fuertes. Además, los algoritmos de hash MD5 y SHA se emplean para asegurar la integridad de los datos, en vez del tradicional CRC empleado por SSH1[83.]

OpenSSH y OpenSSL
SSH1 está disponible de forma gratuita para los usuarios a pesar de contener tecnologías patentadas. Con la llegada de SSH2, la licencia fue restringida y ya no se distribuye de forma gratuita. La comunidad open source no contenta con este cambio de licencia, desarrolló su propia alternativa, OpenSSH. OpenSSH es una versión gratuita del protocolo SSH que ofrece la misma funcionalidad que SSH2 pero sin restricciones derivadas de patentes. OpenSSH versión 2 y superiores soportan los dos protocolos de SSH, lo que permite a OpenSSH crear conexiones desde y hacia clientes que soporten uno o ambos protocolos. OpenSSH hace uso de OpenSSL, que es un conjunto de herramientas para implementar los protocolos de red Secure Sockets Layer (SSL v2/v3), Transport Layer Security (TLS v1) y otros estándares de criptografía requeridos por ambos[84]

4.4 ESTRATEGIAS PARA LA PREVENCIÓN DEL DELITO INFORMÁTICO FINANCIERO

En este aparte, se aborda cuáles deberían ser las principales estrategias para prevenir el delito en general y particularmente el delito informático financiero, lo

---

82 DÍAZ ORUETA, Gabriel; ALZÓRRIZ ARMENDÁRIZ, Ignacio., y SANCRISTÓBAL RUIZ, Elio. Procesos y herramientas para la seguridad de redes. España: UNED - Universidad Nacional de Educación a Distancia, 2014. ISBN 978-84-362-6716-7.

83 CONTRERAS y RICO BAUTISTA. Op. Cit.

84 GONZÁLEZ; GÓMEZ-ARRIBAS y LÓPEZ-BUEDO. Op. Cit., p. 12.

cual involucra no sólo aspectos eminentemente técnicos como los analizados en el capítulo anterior, sino también medidas en términos de actualización el marco jurídico legal para combatir y penalizar ejemplarmente a los delincuentes que cometen este tipo de delitos.

Las estadísticas del fraude informático crecen geométricamente con el mismo ritmo en que el uso de la banca electrónica también aumenta en el país. Por igual, las actividades criminales de la ciberdelincuencia afectan a las entidades financieras (clientes y consumidores financieros) que no en pocos casos tienen que asumir las pérdidas producidas por los desfalcos, accesos abusivos a sistemas de información, transferencia no consentida de activos y las suplantaciones de identidad, entre otros, también del riesgo operativo, la afectación a la reputación de las entidades e incluso a la seguridad misma del sistema financiero.

> Se requiere una estrategia integral en que la política anti-criminal sea un componente fundamental que se adecúe a la nueva realidad de los servicios informáticos en línea:
> a) Revisar la legislación, en particular, la ley 1273 de 2009, Ley de Delitos Informáticos, para determinar su pertinencia y adecuación a los retos actuales, probablemente serán necesarios ajustes para hacerla más efectiva. En particular, es importante que se logre una legislación que obligue la divulgación de los incidentes informáticos que pongan en peligro la seguridad e integridad de la información personal y los secretos empresariales.
> b) Capacitar al personal de fiscales y del Cuerpo Técnico de Policía Judicial en la informática en general y las nuevas tecnologías (cloud computing, internet de las cosas, servicios móviles, deep web (internet profunda), criptomonedas y big data, entre otras) para que puedan enfrentar los retos informáticos.
> c) Establecer reglas ciertas y seguras para la prueba digital que permitan claridad sobre la cadena de custodia y agilizar los procedimientos sin detrimento de las respectivas garantías, pero con la presteza que amerita la economía digital.
> d) Incrementar los mecanismos de cooperación internacional como estrategia para combatir esta modalidad transnacional de crimen organizado.
> e) Contribuir con las políticas estatales encaminadas a mejorar la ciberseguridad y ciberdefensa, incluyendo la ratificación del Convenio de Budapest sobre ciberdelincuencia y la creación de la Agencia Nacional de Ciberseguridad.
> f) Llevar a cabo campañas ciudadanas para la prevención del delito informático, así como en las facultades de ingeniería para prevenir a los futuros profesionales respecto de caer en redes criminales.
> g) Coordinar los estándares de seguridad electrónica y digital con la Superintendencia Financiera para prevenir la acción de la ciberdelincuencia y
> h) Coordinar con el sector privado (sector de las TIC, sector real y sistema financiero) respecto de la prevención del ciberdelito así como de la denuncia de las actividades criminales de las que sean víctimas y de las medidas para asegurar la

prueba e informar a clientes y consumidores afectados de manera indirecta por la fuga de información[85]

Con una mayor experticia de los funcionarios de la Fiscalía, apoyados por la voluntad política de la nueva cúpula, gozando de la cooperación internacional adecuada y en armonía con las políticas públicas de ciberseguridad es posible que Colombia pueda enfrentar con éxito a la criminalidad informática del siglo XXI. No queda otro camino si se quiere que los ciudadanos aprovechen realmente los beneficios de la economía digital y de la Sociedad de la Información, se obtengan los frutos debidos de los programas de conectividad, inclusión y emprendimiento digital del Ministerio de las TIC y la ambiciosa agenda de identificación digital para los servicios ciudadanos y de la carpeta digital ciudadana previstas en el Plan Nacional de Desarrollo. Todos estos loables proyectos, esfuerzos presupuestales y programas bandera requieren de la confianza ciudadana respecto de la seguridad, autenticidad, integridad y disponibilidad de la información digital.

---

85 PEÑA VALENZUELA, Daniel. Llegó la hora de tomar en serio los delitos informáticos [en línea]. En: Peña Mancero Abogados, 2016 [revisado el 4 de marzo de 2016]. Disponible en internet: http://www.pmabogados.co/index.php?option=com_content&view=article&id=423:llego-la-hora-de-tomar-en-serio-a-los-delitos-informaticos&catid=64&Itemid=246&lang=es

6. CONCLUSIONES

Del desarrollo de la investigación los Desafíos Técnicos y Jurídicos frente al Ciberdelito en el Sector Bancario Colombiano, se pueden derivar las siguientes conclusiones:

Con el avance e irrupción de las tecnologías de información y la comunicación TIC, en todos los ámbitos de una sociedad global, el ciberdelito informático es cada vez más generalizado, especialmente en campo financiero y bancario, puesto que permite el acceso a grandes bases de datos relacionadas con fondos de ahorro e inversiones no solo de las instituciones financieras, sino de los usuarios que hacen uso de las tecnologías para la realización cada vez más generalizada de transacciones digitales y por medios electrónicos, constituyendo un sector bastante vulnerable en la medida que no existe correspondencia en cuanto a la implementación de seguridad y prevención de riesgos.

Si bien existen protocolos internacionales y convenciones para buscar alternativas de tratamiento judicial a los autores de comisión de delitos informáticos en todos sus niveles, las legislaciones de los países muchas veces están retrasadas en cuanto a la tipificación de nuevos y sofisticados delitos, si a ello se le suma que muchas veces se cometen desde ámbitos externos a la jurisdicción del país o usuario afectado, volviéndose un tema de impunidad por la misma complejidad de su detección y coordinación internacional entre países.

La falta de un protocolo que permita a los países detectar y combatir eficientemente el ciberdelito, especialmente en el campo financiero y bancario, está afectando a las personas, las organizaciones y los Estados del mundo globalizado, al crecer las vulnerabilidades frente a terceros en los sistemas informáticos, la interceptación de mensajes y en definitiva nuevos ámbitos de indefensión de los ciudadanos con respecto a la criminalidad organizada nacional e internacional.

Desde el punto de vista eminentemente jurídico legal, para el caso colombiano, la legislación y el derecho penal existente, está rezagado en cuanto al establecimiento del castigo ejemplar de penas, al carecer de equipos de investigación con experticia y por otra parte, la tipificación de los delitos a la luz del actual Derecho Penal, dista de contemplar nuevos delitos dentro de la complejidad de su comisión no solo nivel de las fronteras nacionales sino desde otros contextos internacionales, dejando al Estado incompetente para su castigo y penalización.

Los protocolos de seguridad de las entidades financieras en general y del sector bancario en particular, necesitan de un tratamiento permanente en cuanto a investigación e inversiones considerables en equipos, redes y software especializado, sin embargo, las entidades bancarias no siempre están a la vanguardia con los últimos avances tecnológicos, lo cual aumenta la vulnerabilidad de su seguridad y con ello se hace extensiva a los usuarios, donde los riesgos aumentan, pero la contención no solo técnica sino también jurídica no favorecen el castigo ejemplar para los delincuentes que comenten este tipo de delitos.

REFERENCIAS

AGENCIA EFE. El 98,5 por ciento de los riesgos bancarios en América Latina son informáticos [en línea]. 15 de octubre de 2015 [revisado el 2 de marzo de 2016]. Disponible en internet: https://www.efe.com/efe/america/economia/el-98-5-por-ciento-de-los-riesgos-bancarios-en-america-latina-son-informaticos/20000011-2738875 .

ANTONESCU Mihail y BIRĂU, Ramona. Emerging Markets Queries in Finance and Business. Financial and Non-financial Implications of Cybercrimes in Emerging Countries. En: Procedia Economics and Finance. 2015; no. 32, p. 618-621.

BANCO DE LA REPÚBLICA. El Sistema Financiero Colombiano: Estructura y evolución reciente. En: Revista del Banco de la República. 2013. Vol. LXXXVI, no. 1023.

CARBAJAL, Mauricio, RIVERA ZÁRATE, Israel; MARTÍNEZ RAMÍREZ, Adrián; BARRÓN, Erika Rocío; RIVERA, Luis Arturo y PADILLA GODÍNEZ, Fausto Israel. Introducción a la Seguridad con IP Seguro en Internet (Ipsec). En: Polibits. 2005. no. 32. P.16-21.

CARRILHO NEGAS, Mario F.; MARTINHO LOPES, José M. y ROSARIO NEGAS Elsa I. Homebanking users and more relevant security risks associated. En: Iberian Conference on Information Systems and Technologies, CISTI. 2013. p. 1-6.

CONTRERAS, Josue Lobo y RICO BAUTISTA, Dewar Willmer. Implementación de la seguridad del protocolo de Internet versión 6 [en línea]. En: REVISTA GTI. 2012. vol. 11, no. 29. Disponible en internet: http://revistas.uis.edu.co/index.php/revistagti/article/view/2815

CORTE SUPREMA DE JUSTICIA. Sala de casación penal nº 42724 de 11 de febrero de 2015

DE LA MATA BARRANCO, Norberto y HERNANDEZ DIAZ, Leyre. Los delitos vinculados a la informática en el Derecho penal español. En: Derecho penal informático. 2010, p. 159-200.

DE LUARCA, M y SAAVEDRA, J. Delitos contra el patrimonio: La Ley; 2007.

DIAZ GÓMEZ, Andrés. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. En: Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR. 2010. No. 8, p. 169-203.

DÍAZ ORUETA, Gabriel; ALZÓRRIZ ARMENDÁRIZ, Ignacio., y SANCRISTÓBAL RUIZ, Elio. Procesos y herramientas para la seguridad de redes. España: UNED - Universidad Nacional de Educación a Distancia, 2014. ISBN 978-84-362-6716-7.

FARALDO CABANA, Patricia. Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática. En: Eguzkirole. Cuaderno del Instituto Vasco de Criminología. 2007. no. 21, p. 33-57.

FLORES PRADA, Ignacio. Criminalidad informática: aspectos sustantivos y procesales. Madrid-España: Tirant Lo Blanch, 2012.

FLORES SALGADO Lucero. Derecho informático. México, D.F.: Grupo Editorial Patria, 2014.

GANDINI, Isabella. Ley de Delitos Informáticos en Colombia [en línea], 2010 [revisado 2 de marzo de 2016]. Disponible en internet: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia.

GARCÍA GARCÍA-CERVIGÓN, Josefina. El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. En: Icade Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales. 2008, no. 74, p. 289-308.

GARCÍA NOGUERA, Isabel. La reforma penal de la falsificación, tráfico y uso ilícito de tarjetas bancarias. En: IDP: revista de Internet, derecho y política. 2007. No. 5, p. 93-107.

GIMENEZ GARCÍA. Joaquín. Delito e informática: algunos aspectos de derecho penal material. En: Eguzkilore: Cuaderno del Instituto Vasco de Criminología. 2006, no. 20, p. 197-215.

GÓMEZ VIEITES, Álvaro. Auditoría de seguridad informática. Madrid: RA-MA Editorial, 2014

GONZÁLEZ RUS, Juan José. Delitos contra el patrimonio y contra el orden socioeconómico (V). Las defraudaciones. La estafa. En: Sistema de Derecho Penal Español, Parte Especial. Madrid: Dykinson, 2011, p. 481-511.

GONZÁLEZ, Iván; GÓMEZ-ARRIBAS, Francisco. J. y LÓPEZ-BUEDO, Sergio. Implementación de SSH sobre un Sistema Auto-Reconfigurable [en línea]. En: VI Jornadas de Computación Reconfigurable y Aplicaciones, JCRA 2006. Cáceres, Universidad de Cáceres Septiembre 12-14, 2006. Disponible en internet: http://hdl.handle.net/10486/667396

GRISALES PÉREZ, Giovanni S. Análisis dogmático de las conductas de hurto por medios informáticos y semejantes (art. 269i) y transferencia no consentida de activos (art. 269j) Ley 1273 de 2009 [en línea]. Medellín: Universidad EAFIT. 2013 [revisado el 3 de marzo de 2016]. Disponible en internet: https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf?sequence=1

HERNÁNDEZ DÍAZ, Leyre. El delito informático. En: Eguzkilore: Cuaderno del Instituto Vasco de Criminología. 2009, no. 23, p. 227-243.

JAVATO MARTÍN, María. Las tarjetas de crédito y débito: aspectos penales. En: Cuadernos de la Cátedra de Seguridad Salmantina. 2013, no.10, p. 1-31.

KATZ, Matías David. Redes y Seguridad. México: Alfaomega Grupo Editor, 2013. ISBN 9788426719799

LÓPEZ PIMENTEL, Juan Carlos y MONROY, Raúl. Formal Support to Security Protocol Development: A Survey. En: *Computación y Sistemas.* 2008. no. 12. p. 89-108.

MANJARRÉS, Iván, JIMENEZ TARRIBA, Farid. Caracterización de los delitos informáticos en Colombia [en línea]. En: Revista Pensamiento Americano. 2014 [revisado 2 de marzo de 2016]. vol. 5, no. 9, p. 71-82. Disponible en internet: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

MIRÓ LLINARES, Fernando. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid- España: Marcial Pons, 2012.

OJEDA, Jorge Eliecer, *et al*. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. 2010. vol. 11, no. 28, p. 41-66.

PALAZZI, Pablo A. Los delitos informáticos en el Código Penal. Buenos Aires: Abeledo-Perrot, 2009.

PEÑA VALENZUELA, Daniel. Llegó la hora de tomar en serio los delitos informáticos [en línea]. En: Peña Mancero Abogados, 2016 [revisado el 4 de marzo de 2016]. Disponible en internet: http://www.pmabogados.co/index.php?option=com_content&view=article&id=423:llego-la-hora-de-tomar-en-serio-a-los-delitos-informaticos&catid=64&Itemid=246&lang=es

PORTAFOLIO. Denuncias de Ciberdelitos crecen Al 25 % en Colombia, octubre 30 de 2015 [revisado 3 de abril de 2016). Disponible en internet:

http://www.portafolio.co/economia/finanzas/denuncias-ciberdelitos-crecen-25-colombia-26308

POSADA MAYA, Ricardo. El delito de transferencia no consentida de activos [en línea]. En: Revista de Derecho, comunicaciones y Nuevas Tecnologías. 2012 [revisado 1 de marzo de 2016], no. 8, p. 4-27. Disponible en internet: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics120.pdf

QUINTERO CHAPARRO Sandra R y SUÁREZ LEÓN Sandra P. Comisión de conductas punibles en el internet en Colombia. Bogotá: Universidad Militar Nueva Granada, 2012.

RODRÍGUEZ ARBELÁEZ, Juan David. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación [en línea]. 2014 [revisado 1 de marzo de 2016]. Disponible en internet: http://bdigital.ces.edu.co:8080/repositorio/handle/10946/1334.

RODRÍGUEZ ZÁRATE, Alejandro. Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos [en línea]. En: Universitas, 2015 [revisado 3 de marzo de 2016], no. 128. p. 285-314. Disponible en internet: http://revistas.javeriana.edu.co/index.php/vnijuri/article/view/10176/8357.

SALAZAR, Juan F. Situación normativa de la Sociedad de la Información en Colombia. En: Criterio Jurídico. 2011. vol. 9, no. 1, p. 89-103.

RESUMEN ANÁLITICO RAE

Título de Documento.	Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario Colombiano.
Autor	GUERRERO LOZANO, Balvina CASTILLO CAICEDO, Dirley Piedad
Palabras Claves	Desafíos técnicos, desafíos jurídicos. Ciberdelito, Sistema bancario en Colombia, Vulnerabilidades, Amenazas, Legislación, Código penal, Riesgos, Asobancaria, software malicioso, Cracker., Hacker, Internet.
Descripción Desarrollar este estudio monográfico, representa una oportunidad para el fortalecimiento de una de las funciones sustantivas de educación superior: la proyección social y la intervención en el campo del ciberdelito, especialmente la estafa financiera o la movilidad de activos sin consentimiento, mediante generación de nuevo conocimiento, base fundamental para ahondar en futuras investigaciones en un campo tan complejo y cambiante como los sistemas en el contexto de una economía más globalizada.	
Fuentes Bibliográficas	FLORES PRADA I. Criminalidad informática: aspectos sustantivos y procesales. Madrid-España: Tirant Lo Blanch; 2012. GANDINI, I. «Ley de Delitos Informáticos en Colombia.» 2010. http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia (último acceso: 02 de 03 de 2016). GRISALES PÉREZ G.S. Análisis dogmático de las conductas de hurto por medios informáticos y semejantes (art. 269i) y transferencia no consentida de activos (art. 269j) ley 1273 de 2009 [recurso electrónico]. 2013. HERNÁNDEZ DÍAZ L. El delito informático. Eguzkilore: Cuaderno del Instituto Vasco de Criminología. 2009(23):227-43. MENDEZ ALVAREZ, Carlos Eduardo. Metodología: Diseño y desarrollo del proceso de Investigación con Énfasis en

	Ciencias Empresariales. 4a. Edición. Bogotá: Limusa Noriega Editores, 2006

Contenido

Descripción del problema

Los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en el sistema bancario en Colombia, lo cual merece un análisis de contexto sobre los principales desafíos de carácter técnico y jurídico para hacer frente al ciberdelito financiero. Las bondades y los impactos de las TIC y el Internet en los ámbitos económico, político, social, cultural y medioambiental, han generado una serie de efectos negativos como el llamado ciberdelito o delito informático que abrió un amplio campo de riesgos y de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con la seguridad informática, la auditoría de sistemas o auditoría informática. El desarrollo y el impacto de las Tecnologías de la Información y las Comunicaciones (TIC) han generado la concomitante necesidad de ajuste de muchas de las formas de operación y de gestión de las organizaciones, tanto de los procedimientos y estándares de las ciencias y otras tecnologías, como de la interpretación del mundo, sus culturas y paradigmas; y de esa tendencia no se excluye el Derecho, el cual debe incorporar las nuevas tendencias y formas de tipificación de delitos cometidos a través del ciberespacio, pero también la organización que debe incorporar sofisticados procesos de seguridad informática para hacer frente al ciberdelito de carácter nacional e internacional, como afirma Ojeda. Como afirma Miró, actualmente las organizaciones, los Estados y la comunidad internacional son beneficiarios directos de la revolución de las TIC en todos los ámbitos del quehacer humano, pero debido al tratamiento de la información, su intercambio y comunicación en la sociedad actual, también sufre los efectos negativos del cibercrimen, lo que supone que la delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas y por lo tanto, la seguridad informática en términos físicos y logísticos que deben implementar las organizaciones junto al marco jurídico de los Estados y los Organismos Internacionales, constituye una problemática que merece ser analizada y tratada de manera prioritaria. Las organizaciones, los gobiernos y los Estados a través del Derecho y el marco jurídico de cada país, debe enfrentar no sólo a nivel interno sino a nivel global la posibilidad de frenar y castigar la comisión de delitos que afecte la relación de las personas, las organizaciones y la sociedad en general. Hay necesidad, por tanto, de regular el uso del ciberespacio con normas no sólo técnicas, ni tampoco únicamente con códigos de conducta voluntarios, sino con normas jurídicas

eficaces y vinculantes que garanticen los principios y valores de los modernos ordenamientos jurídicos. También la necesidad de superar la dificultad de regular el ciberespacio, más en concreto, de tipificar penalmente las conductas que deben ser sancionadas en el ciberespacio. Con base en Flórez se puede afirmar que los nuevos retos y nuevos problemas que conlleva la existencia del ciberespacio y el Internet como medio de comunicación ha originado lo que será conocido como «ciberdelincuencia». Según Gómez, por su singularidad con respecto a la delincuencia tradicional, este fenómeno exige una consideración especial por parte del Derecho penal, puesto que la mayor parte de los métodos clásicos, no son los más adecuados por cuanto la diversidad de delitos cometidos en el ciberespacio, muchas veces rebasan la jurisdicción del respectivo Estado y por lo tanto hay necesidad de recurrir a la conformación de verdaderas redes inter estatales para la persecución y castigo.

Objetivo General

Analizar las vulnerabilidades, amenazas y desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario Colombiano.

Objetivos Específicos

- Contextualizar la tipificación del delito informático financiero y su tratamiento por parte de algunos países y organismos internacionales.

- Identificar el delito informático financiero cometido al sistema bancario y su tratamiento penal dentro del actual marco jurídico legal colombiano.

- Analizar la seguridad informática del sistema bancario en términos de los desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano.

- Formular recomendaciones, con base en los resultados del estudio, para la prevención del delito informático en el sector bancario colombiano.

Resumen proyecto

El proyecto está delimitado exclusivamente al Sistema Bancario Colombiano, el comprende análisis de las estadísticas de los principales ciberdelitos cometidos durante el periodo 2015 hasta lo corrido del año 2016, según información del ASOBANCARIA, el gremio más importante que agrupa a bancos y entidades financieras, quienes más han realizado innovaciones tecnológicas para garantizar la seguridad informática, sin embargo, han sido las instituciones más afectadas junto con los usuarios por la ciberdelincuencia, por lo tanto, el alcance del proyecto se circunscribe a identificar las vulnerabilidades, amenazas y desafíos técnicos y jurídicos a que se ve enfrentado el sistema bancario colombiano.

Metodología

El presente trabajo se enmarca dentro de un tipo de investigación descriptiva, considerando el nivel de profundidad con que se aborda el proceso investigativo.

En cuanto a diseño de investigación monográfica y atendiendo un esquema de averiguación que hace referencia a la forma como se produjo un nuevo conocimiento sobre el proyecto investigativo mediante un proceso riguroso de adquisición, organización, sistematización y divulgación (teórica y reflexiva) del conocimiento, partiendo de lo simple a lo complejo, de las causas a los efectos, de las partes al todo, de los principios a las consecuencias, de allí los procesos inductivos, de lo particular a lo general y procesos deductivos, de lo general a lo particular, serán los empleados para esta investigación.

Conclusiones

Con el avance e irrupción de las de las tecnologías de información y la comunicación TIC, en todos los ámbitos de una sociedad global, el ciberdelito informático es cada vez más generalizado, especialmente en campo financiero y bancario, puesto que permite el acceso a grandes bases de datos relacionadas con fondos de ahorro e inversiones no solo de las instituciones financieras, sino de los usuarios que hacen uso de las tecnologías para la realización cada vez más generalizada de transacciones digitales y por medios electrónicos, constituyendo un sector bastante vulnerable en la medida que no existe correspondencia en cuanto a la implementación de seguridad y prevención de riesgos.

Los protocolos de seguridad de las entidades financieras en general y del sector bancario en particular, necesitan de un tratamiento permanente en cuanto a investigación e inversiones considerables en equipos, redes y software especializado, sin embargo, las entidades bancarias no siempre están a la vanguardia con los últimos avances tecnológicos, lo cual aumenta la vulnerabilidad de su seguridad y con ello se hace extensiva a los usuarios, donde los riesgos aumentan, pero la contención no solo técnica sino también jurídica no favorecen el castigo ejemplar para los delincuentes que comenten este tipo de delitos.

Recomendaciones.

Se deben endurecer las penas en derecho penal sobre el ciberdelito financiero, para poder enjuiciar a personas de bandas dedicadas a delitos informáticos.

Se deben definir protocolos de seguridad a través de las redes de Internet, los cuales son medios de comunicación e interacción para las transacciones financieras y el intercambio de información entre usuarios y entidades y así crear seguridad y confianza para, garantizar su confidencialidad, integridad y disponibilidad.