COLEGIO UNIVERSITARIO DE ESTUDIOS FINANCIEROS

Máster Universitario en Derecho Bancario y de los Mercados e Instituciones Financieras

Trabajo de Fin de Máster

Tema: La Responsabilidad Civil ante la Seguridad de las Transacciones Electrónicas Bancarias.

Autor:
Verónica Fernanda Monar Gaibor

Tutor:
Dr. José David Ortega Rueda

Madrid, a 13 de septiembre de 2019

ÍNDICE

ÍNDICE DE ILUSTRACIONES Y GRÁFICOS

INTRODUCCIÓN

El proverbio latino *tempora mutandur* significa que los tiempos cambian y el hombre cambia con ellos. La sociedad ha ido evolucionando con el pasar de los años. Desde la agricultura, la revolución industrial hasta llegar a la era de la tecnología y con estos avances los seres humanos nos hemos adaptado, modificado nuestros comportamientos sociales y la forma de gestionar nuestra vida. Por ende, también las estructuras bancarias han sufrido una gran transformación.

La presente investigación tiene como objetivo el análisis de la responsabilidad civil ante la seguridad de las transacciones electrónicas bancarias, ya que en esta relación banca cliente, de sus estructuras, los agentes externos de comercialización han logrado un proceso gradual pero acelerado e imparable de nuevos elementos que afectan a la seguridad jurídica de estas transacciones.

Como primer elemento de este trabajo desarrollaremos las nociones generales de la responsabilidad civil, iniciando con una breve reseña histórica y continuando con conceptos doctrinales y de la legislación española como ecuatoriana. En este primer capitulo, además de las oportunas conceptualizaciones, también hablaremos brevemente y de forma general de la responsabilidad del sector bancario.

La Banca no solo ha tenido que superar su relación banca-cliente, sino que también su estructura interna y con los agentes externos de comercialización y de control. La razón reside en que, para el desarrollo de la tecnología, se le ha vuelto imposible a la banca asumir con inmediatez, los diversos y divergentes campos de actuación. Por ello abordaremos las distintas formas de comercialización de los servicios financieros, y la responsabilidad ante la seguridad al presentarse diversos riesgos en las transacciones electrónicas tales como como el Phishing, suplantación de identidad y la seguridad jurídica en las transacciones electrónicas, etc.

No en balde, la tecnología no solo ha traído una infinidad de avances, mejoramiento de acceso a la información, nuevos servicios, eficiencia y agilidad, sino que también ha acarreado un gran numero de problemas, por este motivo los entes reguladores han tenido que estipular varias exigencias para brindar protección, ante la gigantesca influencia que la tecnología ha tenido en relación con la banca. Por esta razón en nuestro tercer capitulo trataremos de mostrar una manera práctica los sistemas de seguridad que están usando los principales bancos de España y Ecuador, así como analizar cuáles son las diferencias en las realidades sociales de estos países y su implantación de nuevos sistemas de protección.

A su vez, estudiaremos cuáles son los límites de la responsabilidad tanto del Banco como de los usuarios bancarios. Los sistemas bancarios, en un futuro llenos de innovación, deberían afrontar nuevos productos y servicios, y la tarea de los juristas será delimitar por medio de una regulación adecuada y dinámica los mecanismos de seguridad y protección tanto para los agentes bancarios como para los clientes.

Por último, realizaremos un breve análisis de cuales es el riesgo a nivel mundial de los ataques electrónicos, enfocándonos en España y Ecuador, que nos mostraran de forma estadística si es necesario o no la contratación de un seguro bancario como el que ya han contratado algunos bancos a nivel mundial. Con esto damos una noción general de lo que implica para las instituciones el aparecimiento de la tecnología que no solo es un beneficio sino también un riesgo que es parte del giro del negocio de estas entidades.

CAPÍTULO 1

1. NOCIONES GENERALES LA RESPONSABILIDAD CIVIL

Antes de comenzar con nuestro estudio sobre la responsabilidad civil, debemos mencionar que es parte de la responsabilidad jurídica que se la puede dividir en civil, penal y administrativa, en este trabajo al tratar de entender la responsabilidad en las transacciones bancarias nos centramos en la responsabilidad civil contractual y extracontractual.

1.1 Análisis Histórico de la Responsabilidad Civil

Desde los sistemas jurídicos más antiguos las sociedades han necesitado de leyes que sirvan como mecanismo de protección y seguridad sobre las actividades que son parte de la vida cotidiana. En estos sistemas jurídicos primitivos nace la responsabilidad civil que es la obligación de indemnizar un daño causado por el autor de este a la víctima que ha sufrido dicho daño, de ahí partirá nuestro breve análisis histórico [1].

Así, en "la retribución o reparación del daño en los sistemas jurídicos primitivos se confundía con la venganza privada ejercida por la familia o tribu de la víctima a la tribu o familia causante del daño generalmente a través de una pena corporal" [2].

Por esta razón los primeros contenidos sobre la responsabilidad se encuentran en la Ley del Talión que tenía como fundamento la proporcionalidad entre el daño que se causaba y la pena que sería infringida al causante, así lo señala la celebre frase "ojo por ojo, diente por diente"[3].

Ahora bien, se encontraba esta responsabilidad en otros ordenamientos de la antigüedad como el caldeo-asirio-babilónicos, siendo paradigma el Código de Hammurabi y, por el otro lado, los hindúes persas, con el mosaico del Pentateuco, en la que se confundía la noción del delito y pecado debido al régimen teocrático imperante de Israel, y las Leyes de Manú, del Derecho hindú en que predominaba un sistema de responsabilidad objetiva, el resarcimiento de los daños estaba fuertemente vinculado a un componente religioso [4].

Pero para acercarnos más a nuestro concepto actual de responsabilidad debemos establecer que fue el sistema griego el pionero en establecer el concepto de culpabilidad, que más tarde se traslado al sistema jurídico romano, considerando la conceptualización

[1] Yáguez, R. (1993). *Tratado de Responsabilidad Civil*. Navarra: *Revista Jurídica Navarra*, pág.13.
[2] Rosal, J. (1959). *Lecciones del Derecho Penal Español.* Madrid: Lecciones, pág. 180.
[3] Antón, J. Rodriguéz, J.(1949) *Derecho Penal.* Madrid : Camargo Hernández, pág.41.
[4] Quintano, A. (1963). *Curso de Derecho Penal*. Madrid: pág. 90.

griega que, a consecuencia de la libertad, el hombre debía responder moral, social y jurídicamente [5].

Por medio del sistema griego, posteriormente se traslada al derecho Romano, su normativa se la aglomero en las Doce Tablas o también conocida como Ley decenviral. Y así los romanos en los años siguientes ya habían reconocido como la *delicta* como actos lícitos y los *contractus* como actos obligatorios y es en la época del emperador Justiniano del siglo VI d.C que el conceptos en materia responsabilidad se estableció una subdivisión como delictual y contractual y las obligaciones fueron clasificadas en cuatro: delito, cuasidelito, contrato y cuasicontrato, esto en la recopilación de las constituciones imperiales que formaría el Código Justiniano y es así que el Derecho romano establece el concepto de responsabilidad para responder ante ciertos actos, que se genera en base a las relaciones contractuales.

Estos conceptos y premisas fueron asumidos también por el Código Napoleónico de 1804, y que sería también la base de la creación del Código Civil Español que iniciaría con el proyecto codificador realizado por Florencio García Goyena que el 5 de mayo de 1851 se elaboraría por la comisión que durante 5 años y que después de otros ante proyectos como el de 1882 culminaría finalmente con su aprobación del primer Código Civil de España en 1889.

A vez Andrés Bello un jurista venezolano que ayudo a la creación de varios códigos civiles de hispoamérica se basó en el Código Civil Napoleónico y crea los Códigos Civiles chileno y ecuatoriano este último fue aprobado el 21 de noviembre de 1857 y comenzó a regir a partir del 1 de enero de 1861, encontrándose aún vigente.

La influencia del Código Civil napoleónico también se extendió a los Países Bajos, Luxemburgo e Italia, la excepción se halla en el derecho inglés y americano, que se basa en los precedentes judiciales a través del Common Law, por lo que la metodología es diferente a los países con influencia germánica románica. La responsabilidad objetiva en Inglaterra fue reconocida en el caso de Ryland v. Fletcher en 1860 y fue un caso sobre daños y perjuicios como consecuencia de la tenencia de un estorbo privado- privado nuisance, que es la negligencia para imponer responsabilidad por daño. Mientras en Estados Unidos al haber sido colonizada por Inglaterra también su sistema judicial lo adapto y lo hizo propio [6].

Es importante hacer mención de la integración europea que, tras la Segunda Guerra Mundial y en virtud de las ideas integracionistas de Robert Schuman dio a inicio a lo que hoy se conoce como Unión Europea. Es importante tratarla ya que la legislación española

[5] Sarrión, A. (1992). *La Evolución del Derecho de años.* Barcelona: Ponencias y coloquios en la Jornada de Derecho de Daños. pág. 21.
[6] Santiago, C. (2015). *La responsabilidad civil extracontractual de los empresarios.* Madrid: Dyskinson. pág. 21.

se debe a una legislación supranacional que la rige al igual que todos sus países miembros. Es así como para ejemplificar la responsabilidad civil mencionaremos que el Tratado de Maastricht eleva la protección de los consumidores, o así el tratado de Ámsterdam.

Para culminar con este breve análisis histórico sobre la responsabilidad civil podemos entender que es un tema esencial en las legislaciones del mundo, forma transversal de la cotidianidad de las sociedades. Su concepto prevalece desde antigüedad la actualidad hasta nuestros días. Garantiza que los actos propios y ajenos, si causan un perjuicio permiten que la parte afectada pueda acudir a las leyes que compensen y responsabilicen por ese hecho. Y que no exista como en las sociedades antiguas la toma de justicia por mano propia saltando las normas que tratan de ser proporcionales ante el perjuicio causado.

1.2 Conceptos de Responsabilidad Civil

El concepto de Responsabilidad es uno de los más utilizados por las sociedades y no solamente en el ámbito jurídico, sino también en los actos cotidianos de los seres humanos. Desde la responsabilidad estatal, de pareja, en el trabajo, tienen como elemento la identificación de quien fue el responsable de un acto. Así, en un término general la responsabilidad es "la obligación de asumir las consecuencias de un hecho, acto, conducta."[7].

Hart este filosofo del Derecho británico señalaba que la responsabilidad podía ser moral o jurídica, en este trabajo de final de master nos centraremos en la ultima y en la subdivisión en el ámbito civil.

La etimología de la responsabilidad deriva del latín responde, es ere compuesto de re y spondeo, es, ere que es traducible como estar obligado; se trata de una voz anfibológica, dadas sus diversas interpretaciones, cuales son: i) calidad de responsable; ii) deuda, obligación de responder; iii) cargo u obligación moral que resulta del posible yerro o cosa o asunto determinado; iii) capacidad existente de todo sujeto activo de derecho para reconocer y aceptar las consecuencias de un acto suyo inteligente y libre [8].

Además, algunos juristas han analizado el término correcto al que se refiere la responsabilidad civil, así que algunos autores consideran que el término "reparación" es más claro que el de responsabilidad, otros sostienen que el "responder" el que debe utilizarse finalmente, los que señalan que el "derecho de daño" es el más apropiado por que garantiza la reparación de intereses colectivos [9].

[7] Martínez, G. (1998). *Responsabilidad Civil Extracontractual en Colombia.* Medellin: Temis. pág. 3.
[8] Real Academia Española. (1999). *Diccionario de la Lengua española.* Madrid: España Calpe. pág. 1789.
[9] Cordobera, L. (1993). *Los Daños Colectivos y la Reparación.* Buenos Aires: Editorial Universidad. pág.45

En este trabajo de estudio nos regiremos al término de responsabilidad civil siguiendo la línea tradicional que basa su idea que existe una libertad del sujeto y esto conlleva una responsabilidad de cualquier efecto dañoso que causare por el hecho de hacer o no hacer.

Cuando hacemos mención de la responsabilidad jurídica es el acto de hacer responsable a un sujeto por un daño que se a producido en contra de una persona ya sea física o jurídica o ante un bien jurídico protegido. Esta se diferencia de la responsabilidad moral ya que en la responsabilidad jurídica existe una norma que cautela los actos de hacer o no hacer y con esto trae una imputación por el daño causado mientras que la moral responde a un fuero interno.

Pascual Estevil explica esto de una forma más general, al señalar que ser responsable significa afrontar las consecuencias del incumplimiento de una obligación que se hubiere dejado preestablecida es decir responder genéricamente a la violación del principio alterum non laedere lo cual constituye la piedra medular del instituto de la responsabilidad ya que significa el deber de no dañar a nadie consagrada por el jurista romano Ulpiano[10].

Para dar un concepto sobre la responsabilidad Civil el jurista colombiano Gilberto Martinez Rave la define como "La obligación de asumir las consecuencias patrimoniales de un acto, una conducta o un hecho" [11].

Para establecer un concepto nuestro podemos decir que responsabilidad civil lo que trata es de verificar el supuesto de culpabilidad que una persona natural o jurídica ha realizado contra otra, verificando que el hecho haya generado un daño y que exista un nexo entre la conducta y el menoscabo causado, para que exista una reparación al perjuicio. Además, para centrarnos en el ámbito bancario, esta relación de tres elementos de la responsabilidad también se debe aplicar en la relación de la entidad bancaria con el cliente y terceros.

1.3 Responsabilidad Civil Contractual y Extracontractual

Debemos identificar estos dos tipos de responsabilidad para enfocarnos en nuestro trabajo y sobre la actividad bancaría ya que podríamos establecer que la relación banca cliente es exclusivamente contractual, pero en la actualidad por ser un sector multifacético en las todas las actividades subyace una responsabilidad que también puede ser extracontractual. Por esta razón expondremos de que se trata cada una de ellas.

1.3.1 Contractual

Como su nombre lo indica en esta responsabilidad debe existir un contrato de por medio y que exista un incumplimiento de las estipulaciones que se detallen en el mismo, por lo

[10] Estevil, L. (1989). *Hacia un concepto actual de responsabilidad civil.* Barcelona: Boch. Pág.68
[11] Martinez. G. (1998). *Reponsabilidad Civil Extracontractual en Colombia.* Medellin: Temis. 1998. pág. 11.

que se debe probar el vinculo contractual, así también lo señala Javier Tamayo Jaramillo "Para que surja responsabilidad contractual, se requiere que haya un daño proveniente de la inejecución de un contrato válidamente celebrado entre la víctima y el causante del daño" [12].

Así también lo señala el Código Civil Español y Ecuatoriano, que establecen al contrato como uno de las fuentes de las obligaciones y establece en su artículo 1089 que "Las obligaciones nacen de la ley, de los contratos y cuasi contratos…"1091 "Las obligaciones que nacen de los contratos nacen con fuerza de ley entre las partes contratantes…" [13] y el Código Civil Ecuatoriano en su artículo 1453 establece la "Las obligaciones nacen, ya del concurso real de las voluntades de dos o más personas, como en los contratos o convenciones.." [14].

Por esta razón, la responsabilidad civil contractual supone la transgresión de la Ley del Contrato que al no cumplir con una de las disposiciones del contrato esto genera una responsabilidad contractual y por esta razón existe un resarcimiento por el daño causado. Es decir, "Si la obligación generada en la convención es incumplida por el sujeto a darle satisfacción, estaremos en presencia de la responsabilidad contractual"[15].

En el sector bancario podríamos establecer que, en gran medida, se encuentra la relación contractual, el cliente bancario firma un contrato para que el banco le brinde un servicio y, si existe una ruptura o quebrantamiento de *lex privata contratu* que quiere decir la ley privada del contrato se aplica que si causare un daño, entonces habra una responsabilidad de subsanar el daño causado siempre que se pruebe la culpa. Debemos mencionar que en la actualidad los contratos bancarios no solamente son de apertura de cuenta, de uso de tarjeta, sino que en la actualidad existen contratos para la utilización de banca móvil y banca digital.

1.3.2 Extracontractual

Cuando nos referimos a la responsabilidad extracontractual, como su nombre lo indica, no es necesario que exista un contrato, y la obligación nace a pesar de que no exista vinculación previa, de las partes. Todo nace al producir un daño, ya que no todo acto que modifique o incurra una transformación genera responsabilidad civil, debe este hecho causar una afectación a una persona natural o jurídica y vincular a las dos partes.

Pero además de la existencia del daño, se debe probar la existencia de la relación del daño causado con el hecho, nos dice así el Código Civil Español en su artículo 1902 que "El por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado

[12] Tamayo, J. (2007) *Tratado de Responsabilidad Civil*. Ed. II. Bogotá: Legis. Pág. 4.
[13] Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.
[14] Registro Oficial Suplemento 46 de 24-jun-2015. Codificación Del Código Civil del Ecuador.
[15] Rodríguez, G. (2014). *Responsabilidad Contractual.* Chile : Jurídica de Chile. pág. 11.

a reparar el daño causado", pero también en la responsabilidad extracontractual se deberá probar la culpa [16].

Para para hablar sobre la Responsabilidad Civil en España debemos revisar el Código Civil que en su artículo 1902 del Capitulo de las obligaciones que nacen de culpa o negligencia señala "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado" [17].

Es decir, que cualquier daño que genere un tercero existe la responsabilidad de indemnizar si es que hubiera la culpa, que los ordenamientos jurídicos consideran como un requisito indispensable. Y entonces si tomamos en consideración la culpa se establece que nace de un hecho voluntario y consciente, y que no solo es una conducta de hacer sino también el hecho de omitir hacer, y esta ultima en base a si previamente esta establecido un deber de actuar. Por lo tanto, el régimen de responsabilidad civil, en base al Código de España, establece una responsabilidad subjetiva que se imputa en base de la culpa.

El Doctor Acevedo Prada señala que el Código Civil español solo incluyó el régimen general de responsabilidad civil subjetiva y limitó a una regulación particular las situaciones que requieran una aplicación objetiva del régimen de responsabilidad.

También podemos mencionar que en los años ochenta y noventa el Tribunal Supremo Español estipularía en sus jurisprudencias la responsabilidad civil en forma objetiva, así en el STS de 8 de Noviembre de 1990 o de 30 de Diciembre de 1995, pero que después regresaría a su concepción original de la culpa como base de la responsabilidad es decir a un sistema subjetivo con la jurisprudencia STS de 6 de septiembre de 20015, 5 de septiembre de 2007, 21 de noviembre de 2008 [18].

Entonces podemos decir que al considerar el régimen español se puede sintetizar en el brocardo latino *Alterum non laedere* (no dañar al otro), que es el un sistema subjetivo de responsabilidad y ante estas circunstancias nos dice la doctrina española que "el agente responderá por el daño que se ha producido por su culpa. No responderá, entonces quien actuado con negligencia debida. Por tal razón, en el régimen subjetivo deberá la victima probar la culpa del autor" [19].

Por lo que para considerar en nuestro presente tema de estudio a la responsabilidad desde el punto de vista de la legislación española debemos considerar que debe existir la culpa dentro de la conducta realizada y por ende un acto humano, voluntario, doloso o culposo y si se comprueba estos elementos existirá la obligación reparadora del acto.

---

[16] Real Decreto de 24 de Julio de 1889 por el que se publica el Código Civil.
[17] Idem.
[18] Gárdo, A. (2016). *Manual de Derecho de Obligaciones.* Valencia: Dykinson. pág. 83
[19] Yágüez, R. (2008). *La Responsabilidad Civil. Cuestiones Previas de delimitación.* Barcelona: Bosh. pág. 1256

1.4 La legislación Ecuatoriana sobre responsabilidad Civil

Como habíamos señalado en nuestro análisis histórico sobre la responsabilidad civil, debemos comprender que el sistema jurídico de Ecuador tiene una estructura románica germánica y adaptó los lineamientos del Código Napoleónico, así como de las Siete Partidas Alfonso X. Es por esta razón que al igual que el Código Civil Español, heredamos la tesis subjetivista que, como hemos explicado, esta fundamentada en probar el daño causado, el hecho generado pero principalmente la culpabilidad.

Es por esta razón que esta corriente es de aplicación general para la legislación ecuatoriana, el Código Civil del Ecuador señala en su artículo 2214 que "el que ha cometido un delito o cuasidelito que ha inferido daño a otro, está obligado a la indemnización; sin prejuicio de las penas que se impongan las leyes por el delito o cuasidelito"[20].

Como sabemos, el delito o cuasidelito son fuentes de las obligaciones: el delito es considerado como un hecho ilícito realizado con intención, es decir un hecho consiente de dañar u ocasionar un perjuicio; mientras que el cuasidelito es un hecho ilícito que genera una acción dañosa, pero sin que haya la intención de hacer mal. Debemos recordad que estos pueden ser civiles o penales y, en nuestro caso, nos centramos en el ámbito civil.

Es así, que el propio Código Civil Ecuatoriano en su artículo 1453 , señala que Las obligaciones nacen, ya del concurso real de las voluntades de dos o más personas, como en los contratos o convenciones; ya de un hecho voluntario de la persona que se obliga, como en la aceptación de una herencia o legado y en todos los cuasicontratos; ya a consecuencia de un hecho que ha inferido injuria o daño a otra persona, como en los delitos y cuasidelitos; ya por disposición de la ley, como entre los padres y los hijos de familia.

Y a su vez establece el artículo 2184 nos habla del cuasidelito este como un hecho culpable "… pero cometido sin la intención de dañar¨, mientras que el delito". cometido con la intención de dañar¨

Y aunque el Ecuador tiene como base la responsabilidad subjetiva la cual establece que el imputado pruebe la presunción de culpabilidad mostrando que actuó diligentemente para evitar el daño causado existe una excepción sobre esta presunción de responsabilidad dada por el Caso Comité Delfina Torres Vda. De Concha vs PETROECUADOR y otros, por el daño ambiental, en la sentencia dictada por la Corte Suprema de Justicia del Ecuador número 31-2002, establece que se invierte la carga de la prueba.

[20] Registro Oficial Suplemento 46 de 24-jun-2015. Codificación Del Código Civil del Ecuador.

Es por esta razón que, al igual que en la legislación española la ecuatoriana lo que interesa probar la existencia del daño causado que por si solo no genera responsabilidad, sino que es la culpa es aquella que muestra el factor de atribución subjetivo de la responsabilidad.

1.5 La Responsabilidad Civil en la Banca

Cuando pensamos en el sector bancario debemos entender que, por sus múltiples actividades, la responsabilidad puede ser civil, administrativa o penal, ya que no solo financian a las familias, empresas, sino también tienen otros servicios de inversión. Ya que son parte esencial en las sociedades, el incumplimiento de estas obligaciones acarrea una responsabilidad.

En este trabajo nos hemos centrado en la responsabilidad que tienen estos bancos en las transacciones electrónicas, que aunque no se encuentre su regulación materializada por la amplia gama de nuevas tecnologías que se registran a diario, los bancos deben ir asumiendo mecanismos que protejan al cliente de posibles daños.

El Doctor Héctor Ángel Benelbaz nos dice que "en el pensamiento francés la responsabilidad de la responsabilidad financiera es una responsabilidad profesional y especifica y ponen el acento en lo que se considera culpa profesional, una especie de culpa mas incisiva, más puntual y que surge de los mecanismos bancarios" [21].

Como lo explicamos en el concepto de responsabilidad debe tener tres elementos la primera es la culpa de la entidad financiera, segundo el perjuicio al cliente bancario y por ultimo la relación entre la culpa y el perjuicio, pero este concepto lo tenemos claro al considerar las funciones tradicionales de la banca, pero en estos años las modificaciones de esta actividad se han ido expandiendo por la tecnología es ahí donde nos deja el punto de análisis de este trabajo.

Ya que sabemos que la Banca es responsable contractualmente de clientes bancarios, por ende todas las obligaciones que debe cumplir la banca se encuentran estipulados en contratos que firman las partes y en estos existirá las consecuencias del incumplimiento de estos. Pero a su vez, de forma más amplía también será la entidad bancaría responsable del ejercicio de su profesión y si estas causaren un perjuicio a al cliente bancario u a terceros en especial las relacionadas con las de su responsabilidad profesional.

[21] *Responsabilidad de las entidades financieras.* Benelbaz, Héctor Ángel. 2017. s.l.: Revista de la Universidad de Mendoza, 2017.

CAPÍTULO 2

2. SEGURIDAD ON-LINE Y POSIBLES PELIGROS DE LAS TRANSACCIONES ELECTRÓNICAS BANCARIAS.

Con la aparición del internet en 1983 y con la aparición de World Wide Web (conocida por sus siglas WWW) en 1993 marca un hito que da la vuelta de las formas de comunicación, comercio y negociación alrededor del mundo. La globalización de la economía, la masificación de la comunicación y el desarrollo de las redes ha transformado la sociedad industrializada en una sociedad de las tecnologías y la comunicación, como a las que conocemos como TICS.

Mostrando un proceso gradual pero acelerado e imparable a nuevos modelos sociales de organización que han afectado también al sector bancario y financiero, estos han tenido que irse adaptándose de manera creativa para entrar en la competencia económica y la eficiencia organizativa que exigen las nuevas generaciones y la sociedad.

Existen algunas etapas que ha vivido la banca con la aparición de la tecnología, la primera es la implantación de sistemas internos que mejoraron la productividad y permitieron reducir los tiempos del procesamiento de la información. Consecuentemente pusieron a disposición servicios por medio de canales electrónicos para los usuarios bancarios, pero es sin duda en los años noventa donde se implementa por completo canales de comunicación y servicios a través de la red.

Es así que la sociedad y sus nuevas formas económicas siguen evolucionando día a día como nos dice libro de *El futuro de las Fitech* escrito por Susanne Chishti y Janos Barberis en el 2017 cuando hablan sobre el sector bancario señalan que "En el futuro, una vez me haya conectado e mi banca móvil (presumiblemente biometrías cardiacas o reconocimiento fácil) tendré la posibilidad de tomar dinero P2P vía Ratesetter, de hacer un pago internacional usando Transferwise, de cargar mi monedero electrónico de Starbucks o de hacer un ingreso en mi fondo de inversión Alibaba". Esto lo decían hace a penas 2 años y sin duda muchas de estas formas de acceso a la banca ya son una realidad en el 2019 [22].

Este cambio social y tecnológico en la banca han hecho que este ultimo sea considerado como un recurso estratégico, pero también esto ha causado varios problemas así el Observatorio Español de Delitos Informáticos muestra que en el año 2017 en España se registran 81307 delitos informáticos, en el 2018 en la ciudad de Madrid existieron 12.169 delitos informáticos y en Andalucía 15.458, sin duda una cifra elevada que se repite alrededor del mundo [23] .

[22] Chishti,S, Janos,B. (2017). *El Futuro es Fintech.* Reino Unido: Jonh Wiley & Son Ltd, pág. 33.
[23] Observatorio Español de Delitos Informáticos. (2019) *Reporte de Ciberdelito en España.* Recurso Online, disponible en «http://oedi.es/estadisticas/». (última consulta 3 de agosto de 2019)

Estos problemas como los ciber crímenes cada día son más sofisticados y la tecnología también. Su impacto representa perdidas millonarias a los bancos y a las economías mundiales, así por ejemplo con la implantación de la tecnología 5G de internet la Agencia de la Unión Europea para la Cooperación Policial (EUROPOL) hace una advertencia sobre que no saben si será posible el rastreo a los delincuentes.

Catherine De Bolle, explico "las redes 5G hacen que el monitoreo de criminales sea mucho más difícil porque dispersan los datos en muchos elementos del sistema" pero también que por la capacidad del 5G por medio de computadoras cuánticas podría ser más fácil el acceso a los sistemas de cifrado [24].

Por esta razón, en este capitulo realizaremos una explicación de cuales son estos ciber crímenes, actos ajenos a las leyes que se generan en la red, siendo de gran preocupación por el gran perjuicio que causan y que a la par de la innovación tecnológica encuentran formas creativas de transgredir los sistemas de seguridad financieros así por ejemplo el Phishing, Pharming, La Suplantación de identidad, Ciberestafa, Craking, Hacking, Vishing, Cross- Pharming – Fake apps son solo algunos de los delitos que se encuentran en el ciber espacio.

Y este es un tema muy sensible para los bancos pues además de crear nuevas herramientas que hagan eficientes sus servicios financieros también deben enfocarse en tener sistemas confiables y de tener estructuras de ciber seguridad para así detener los fraudes financieros que se efectúan a diario en la red.

Por ejemplo, el BBVA tiene 4,6 millones de clientes activos en los últimos 2 años, en los sistemas electrónicos, esto ha traído una mayor vinculación y venta cruzada y transnacionalidad por las nuevas herramientas digitales, más de 42 % de la productividad en la red, eficacia reduciendo los costos de transacción en un -31% en los últimos dos años[25].

Este ejemplo significa que más clientes se encuentran utilizando las nuevas herramientas tecnológica y además que los servicios tecnológicos hacen que sean más eficientes y competitivos.

Pero no es de extrañarnos que las noticias sobre los hackers y sus robos sea titulares, así el Diario Confidencial en el 2015 llamaba en su titular "El ciber-robo del siglo: sacan 1.000 millones de dólares de varios bancos con un troyano", este dinero fue sustraído de

[24] BBC News Mundo. (2019) *Por qué la tecnología 5G hará más fácil perseguir a los criminales*, Recurso Online, disponible en «https://www.bbc.com/mundo/noticias-49064315» (última consulta) 22 de julio de 2019)

[25] Semple.C. (2019) *Los resultados de la transformación digital de BBVA,* Recurso Oline, disponible en « https://www.bbva.com/es/bbvas-digital-transformation-delivering-the-results/» (última consulta) 21 de julio de 2019)

100 entidades financieras pero hace pocos meses se llevo a cabo un ataque al sistema del Far Easter International Bank, que desde sus servidores hasta su terminal SWIFT fueron afectados y se lograron llevar 60 millones de dólares [26].

Otros ejemplos de grandes ciber atracos son Banco del Austro de Ecuador lograron robar 9 millones de dólares, Banglasdesh Bank que en febrero de 2016 por medio de un ataque malware se realizó una transferencia por un valor de 951 millones de dólares, lo que tuvieron en común estos ciber ataques es que se lo realizó a través de la red SWIFT (Sociedades para las Comunicaciones Interbancarias y Financieras Mundiales).

Estas amenazas y la desprotección de los sistemas bancarios la confirman la Security Report 2018 Check Point señala que existen tres puntos esenciales que amenazan al sector financiero y son las ofensivas contra la red SWIFT, el malware que ataca a la banca móvil y el robo de información. Y que los bancos deben integrar soluciones avanzadas para desarrollar su ciberseguridad de sus sistemas internos como de las nuevas apps que utilizan sus usuarios.

2.1 Seguridad on-line

El uso de nuevas tecnologías implica riesgos y perdidas millonarias a los sistemas bancarios y a las economías a nivel mundial, es así como existe todo un desarrollo de seguridad on-line. Para definirla podemos decir que son todas las técnicas, herramientas, políticas, acciones, seguros, normativa y procedimientos que intentan resguardar a todo sistema on-line de posibles ataques. Entonces estos sistemas tratan de buscar herramientas de prevención, detención, respuesta y remediación ante posibles ataques.

Estos sistemas de protección de datos se van desarrollando de manera ingeniosa, dinámica para contrarrestar los ciberataques que se generan a diario en las entidades bancarias. Aunque sin ser estos esfuerzos suficientes. Así las empresas de servicios financieros afirman que sufren 300% más ataques que el resto de las empresas.

Los bancos destinan millones de dólares para el desarrollo de ciber seguridad, ya que un pequeño fallo en esta puede traer consecuencias económicas como sociales sin precedentes. En el informe de Kaspersky Lab dice “que un incidente de servicios de banca electrónica tiene un coste promedio para la entidad financiera de 1,6 millones de euros, un poco más del doble del coste de recuperación ante un incidente de malware, que suele llegar a alcanzar los 750 mil euros” [27].

---

[26] Brunat. D. (2015) *El Ciber-Robo del Siglo.* Recurso Oline, disponible en: « https://www.elconfidencial.com/mundo/2015-02-17/el-ciber-robo-del-siglo-sacan-mil-millones-de-dolares-de-varios-bancos-con-un-troyano_713592/ » (última consulta: 13 de agosto de 2019)

[27] Expansión. (2017) (10 de julio de 2017). *Cada incidente de seguridad online supone para la banca una factura media de 1,6 millones de euros.* Recurso Online, disponible en «https://www.expansion.com/economiadigital/companias/2017/07/23/596ca65d22601dbe118b456b.html » (última consulta: 14 de agosto de 2019)

Pero no solamente existe la perdida económica, sino trae consigo un sin numero de otros problemas para una entidad financiera. Un ejemplo es la perdida de la reputación, o la perdida de datos y es por esta razón que bancos contratan seguros para protegerse ante los eventuales riesgos como por ejemplo Bankia contrato uno con American International Group (AIG) que cubre las operaciones de sus 2,37 millones de clientes [28].

El informe de "Paymets fraud and control survey report" elaborado por Mogarn Chase, nos dice que los malware cada vez son más sofisticados y las técnicas de ataque están también evolucionando[29]. Y no solo los grandes bancos están preocupados por la seguridad, si no también los ciudadanos promedios el 45% que sufren problemas por la perdida de datos y robos a sus cuentas personales. También los gobiernos así por ejemplo el Reino Unido destina 2.300 millones de euros para programas de protección en internet y Estados Unidos 1.500 millones de dólares.

Un estudio realizado por Bussines Insider Intelligence estima que en 2020 se habrán gastado nada menos que 665.0000 millones de dólares en proyectos de seguridad electrónica para proteger ordenadores, dispositivos móviles y dispositivos conectados a internet. Por ejemplo, Caixabank invierte de 300 a 400 millones de euros al año en ciberseguridad, que es una elevada suma en su gasto administrativo [30].

Aunque se destinan miles de recursos económicos, humanos y tecnológicos para crear protección y sistemas bancarios más seguros, las nuevas formas de acceso a los sistemas informáticos hacen que la tarea sea casi titánica ya que existe un ciberespacio común en donde se conjugan miles de usuarios, bancos, empresas y por supuesto criminales del ciberespacio.

2.1.1 Certificado de seguridad

Para centrarnos un poco en lo que es la ciberseguridad, es necesario conocer el certificado de seguridad (SSL) "Secure Sockets Layer o capa de conexión segura es un estándar de seguridad global que permite la transferencia de datos cifrados entre un navegador y un servidor web", que fue creado por Netscape Communications Company propiedad de American Online. Este certificado es un método cifrado que da garantía de navegación valida y segura [31].

---

[28] Bankia Blog (2018) *La ciberseguridad, el gran reto del sector bancario* . Recurso Online, disponible en «https://www.blogbankia.es/es/blog/ciberseguridad-sector-bancario.html» última consulta: 14 de agosto de 2019)

[29] Panda Security. (2018). «Guía de supervivencia contra ciberatracos millonarios» Recurso Online, disponible en «https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/06/Privacidad-Instituciones-Financieras.pdf.» (última consulta: 14 de agosto de 2019)

[30] Bankia Blog (2018) *La ciberseguridad.* Recurso Online, disponible en «https://www.blogbankia.es/es/blog/ciberseguridad-sector-bancario.html» última consulta: 14 de agosto de 2019)

[31] Verising (2019). *Everything You Need to Know About SSL Certificates.* Recurso Online, disponible en «https://www.verisign.com/en_US/website-presence/online/ssl-certificates/index.xhtml?loc=en_US» última consulta: 14 de agosto de 2019)

En el certificado de seguridad existen niveles de seguridad comenzando por el cifrado de datos, la autentificación del servidor, integridad, no repudio. Los tipos de logaritmos de cifrado son diversos así puede ser un cifrado simétrico, asimétrico o hash la diferencia entre estos es que los dos primeros usan claves y el segundo una huella dactilar.

Las entidades financieras se les asigna un certificado SSL con validación extendida y que haciendo un clic sobre "https" o sobre el candado podemos leer quien es el emisor y propietario del certificado. Estos sistemas tienen niveles de validación en el caso de las transacciones bancarias se solicita que tengan elevados niveles de seguridad como el EV-SSL (Extended Validation).

Así, por ejemplo, si entramos a la página web del Banco BBVA y señala que su sistema de protocolo de SSL esta cifrada mediante un algoritmo de 128 bits y es emitida por Google Internet Authority G3 y solicita a sus usuarios verificar que se encuentre en una página del banco con esta validación. Las empresas que brindan estos certificados de SSL son privadas, este este caso la empresa es google Trust Services una LLC.

A su vez hemos realizado el procedimiento de verificación del Banco Pichincha del Ecuador, en este certificado se señala que esta emitido por Digi Cert SHA, Extended Validation Server CA, nos muestra su fecha y hora de caducidad que es el 3 de diciembre de 2019 según la siguiente imagen.

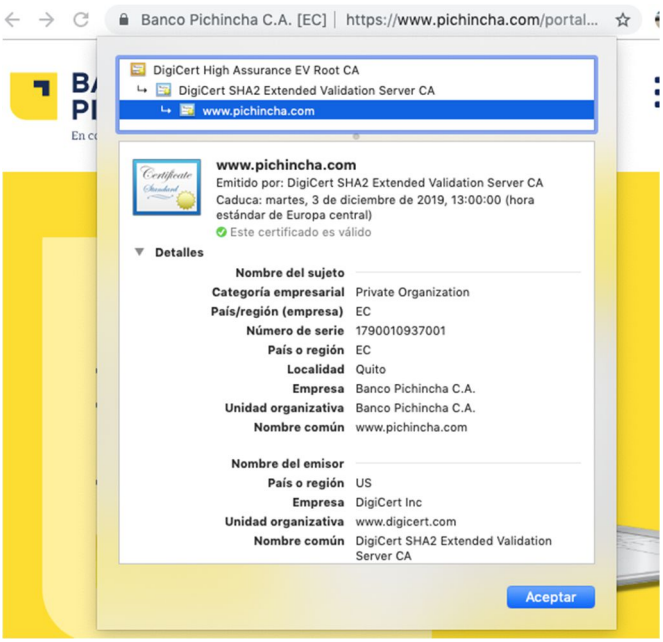

Ilustración 1: Certificado de Seguridad Banco del Pichincha[32]

[32] Banco del Pichincha (2019). *Foto Scream de Pantalla de Certificado Electrónico*. Recurso Online, disponible en «wwww.bancodelpichincha.con» (última consulta 19 de agosto de 2019)

O a su vez el certificado de seguridad del Banco Santander que es emitido por DigiCert SHA2 Secure Server CA y que tiene su fecha de caducidad el 24 de enero de 2020 a las 13h00 según imagen siguiente.

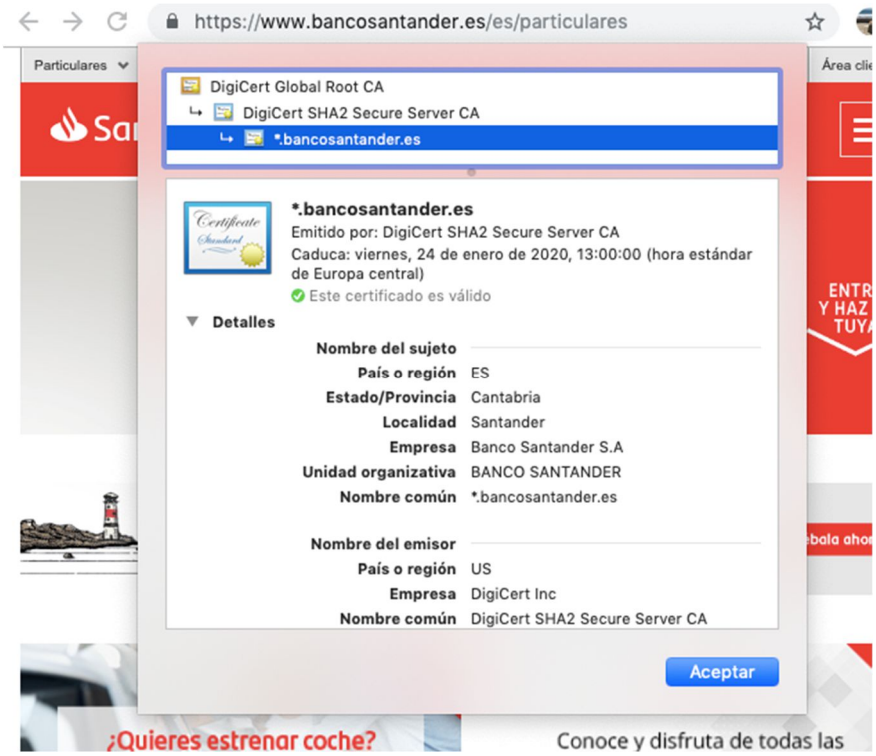

Ilustración 2: Certificado de Seguridad Banco Santander[33]

Este certificado de seguridad puede ser contrato por cualquier persona, empresa o entidad pública o privada la cual garantiza que al navegar dentro de un sitio este sea seguro para los usuarios. Trata de proteger la transferencia de información confidencial en especial en el sector bancario en donde se manejan claves, número de cuentas, gastos, pago de impuestos etc.

2.1.2 *Cifrado de datos*

Cuando pensamos en el cifrado de datos pensamos que es algo muy nuevo, pero en realidad se lo utiliza hace desde hace miles de años y esta basado en la criptografía que comenzó a ser usada por los romanos y griegos que enviaban mensajes confidenciales usando números o letras que tenían combinaciones secretas o claves y que aun seguimos usando en la actualidad para proteger información sensible, por ejemplo uno de los cifrados más conocidos de la edad media es el disco de cifrado inventado por el matemático León Alberti.

[33] Banco Santander (2019). *Foto Scream de Pantalla de Certificado Electrónico*. Recurso Online, disponible en «wwww.bancosantander.es» (última consulta 19 de agosto de 2019)

En la actualidad los cifrados usan los algoritmos que son mucho más complejos, este viene del latín dixit algorithmus que significa número, que son secuencias de pasos lógicos con el fin de solucionar un problema. El primer uso de cifrado con la tecnología lo desarrollo por IBM para proteger información importante del gobierno en 1970 y que después sería creada una versión estándar en Estados Unidos en 1977 [34].

Este puede ser asimétrico que se usa en especial en los correos electrónicos, que por medio de una clave pública el destinatario cifra el contenido del mensaje, mientras el receptor utiliza una llave privada que le da acceso a esta información. Mientras que el simétrico se utiliza una misma clave para el receptor como el destinatario del mensaje. El cifrado conocido como estándar es el DES (Data Encryption Standard) en esta se utilizan bloques de 8 Bytes y una clave de 64 Bits, mientras otros como el DES PUNTO utiliza 64 Bits y una clave de 192 Bits, pero existen cifrados más avanzados como el AES que es un algoritmo de sustitución.

El cifrado de datos se afianzo con la utilización del concepto del derecho a la vida privada y de los datos personales, este mecanismo jurídico toma mayor relevancia desde la segunda mitad del siglo XX y desde entonces varias legislaciones han establecido normativa que precautela este derecho, no solo con instrumentos nacionales sino también supranacionales.

Así por ejemplo en la legislación española existen sujetos o empresas que están obligados a cifrar datos esto según la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales que se aprobó el 22 de noviembre de 2018 que se la crea para adaptar el Reglamento Europeo de Protección de datos y que es de aplicación directa. En el Reglamento Europeo nos dice en su artículo 32 sobre la seguridad del tratamiento numeral 1 letra a) señala:

"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: a) la seudonimización y el cifrado de datos personales;" [35].

A diferencia la legislación del Ecuador que la protección de datos esta en varias normas por ejemplo en la Constitución de la República del Ecuador en su artículo 66 numeral 19 estipular el derecho a la protección de datos de carácter personal o en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que menciona un concepto de datos personales. Pero no existe una ley especifica en relación con este tema.

[34] González, G (2014). *Blogthinkbig.* Recurso Online, disponible en «https://blogthinkbig.com/que-es-el-cifrado» (última consulta: 20 de agosto de 2019)
[35] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Los requisitos de cifrado y protección de datos se encuentran en las resoluciones de la Superintendencia de Bancos del Ecuador por ejemplo en el número SB-2018-945. Por esta razón desde el 16 de enero de 2019 se presenta un anteproyecto "Ley Orgánica de Protección de Datos Personas para Ecuador" que tiene como base la normativa europea presentado por la Dirección Nacional de Registro de Datos Públicos ante la Asamblea Nacional del Ecuador, que se espera que de una estructura jurídica sobre este tema en el Ecuador.

2.2 Concepto de Ciber Crímenes

Los ciber crímenes también son conocidos como delitos informáticos so aquellos que lesionan la seguridad de los sistemas informáticos, poniendo también en peligro otros bienes jurídicos tutelados. Por lo que estos delitos distan de los tradicionales por que su forma de ejecución se los hace por medio de procedimientos electrónicos e informáticos y que su localización se encuentra en el ciberespacio.

Nidia Callegari señala que el delito informático "es aquel que se da con la ayuda de la informática o de las técnicas anexas" [36]. Ahora bien, un concepto más completo nos da el jurista Parker que los define como "Todo acto intencional asociado de una manera u otra a los computadores; en los cuales la victima ha o habría podido sufrir una pérdida; y cuyo autor"[37].

Es por esto por lo que podemos decir que cualquier actividad delictiva que se utilicen medios informáticos, internet es un ciberdelito o un cibercrimen, al igual que un delito común puede ser por acciones u omisiones y debe tener los elementos sine qua non del delito la conducta, tipicidad, antijuricidad, culpabilidad, punibilidad.

Aunque este trabajo no esta destinado a un análisis en el ámbito penal es necesario mencionar que en España la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, establece penas de uno a cuatro años y multa de doce a veinticuatro meses, por la vulneración de la intimidad de un tercero. Esto se encuentra en el artículo 197 y 197 bis, ter. O a su vez en el artículo 248 que señala sobre los fraudes informáticos, o el sabotaje informático que se establece en el artículo 263, etc.

Así también, en el Código Integral Penal del Ecuador establece una pena privativa de la libertad de uno a tres años por la violación a la intimidad en su artículo 178 y en su artículo 190 nos habla de que será la misma sanción por la apropiación fraudulenta por medios electrónicos y en el 229 nos habla de la revelación ilegal de base de datos o en su artículo 231 que señala sobre la transferencia electrónica de activo patrimonial o el 232 que

[36] Velázquez, J. (1996). *El Estudio de caso en las relaciones juridicas internacionales.* Mexico: UNAM. pág, 283.
[37] Romero, C. (2008). *Poder Informatico y Seguridad Júridica*. Madrid:Fundesco, pág.24.

especifica una pena mayor de 3 a 5 años por el ataque a la integridad de sistemas informáticos, etc.

Después de haber establecido conceptos generales sobre los delitos informáticos y ver brevemente la legislación española y ecuatoriana nos centraremos en estos problemas específicos de estas nuevas formas de cometer delitos en el sistema financiero por lo que hablaremos de los siguientes delitos informáticos Phishing, Pharming, La Suplantación de identidad, Ciberestafa, Craking, Hacking, Vishing, Cross- Pharming y las Fake apps.

2.3 Tipos de Cibercrimenes

2.3.1 Phishing

El phishing es un fraude electrónico, se deriva de una palabra ingles que significa pesca, y esto se debe a que lo que intenta es que los usuarios financieros muerdan el anzuelo. Es decir que por medio de anzuelos o trampas intenta obtiene la información de los usuarios. Lo que hacen los delincuentes cibernéticos es estafar para obtener una información confidencial como por ejemplo una contraseña, información bancaria etc.

Los primeros casos de Phishing tuvieron lugar en los 90 por un grupo de hackers que se hacían llamar "The Warez Comminity". Este grupo comenzó creando programas generadores de números de tarjeta de crédito para crear cuentas en AOL. Luego empezaron a hacerse pasar por empleados de AOL para obtener la información de sus clientes a través de la aplicación de mensajería "AOL Messenger", haciendo uso de ingeniería social. Fue en 1996 cuando por primera vez se utilizó el término "Phishing" para referirse a este tipo de estafas. El origen de la "ph" del término Phishing es un tributo al hácking telefónico "Phreaking" [38].

Aquí, el criminal es conocido como phisher o en español estafador envía una comunicación ficticia haciéndola pasar por oficial, esto provoca la confusión del usuario bancario que entrega su información pensando que es un espacio seguro.

La forma en que en general lo realizan es usando la técnica de password harvesting, para tratar de conseguir la contraseña del usuario bancario, para lo cual desde el envió de mails, enlaces falsificados, web falsificadas que suelen ser muy similares a las originales hacen que los usuarios bancarios entreguen información confidencial.

En la actualidad el crecimiento de los ataques por phishing es incalculablemente y ha causado perdidas millonarias a bancos y a clientes, además que cada día las formas de

[38] AndaluciaCERT. (2017). *Centro de Seguridad*, Recurso Online, disponible en «https://www.seguridad.andaluciaesdigital.es/documents/» (última consulta: 21 de agosto de 2019)

confundir a los usuarios son más creativas y casi imperceptibles con métodos muy variados como ingeniería social en donde se trata de hacer pensar a la victima de la legitimidad de la información, o como la falsificación del remitente, o del HTML, o links falsificados, archivos adjuntos etc.

Es decir que existen una multitud de técnicas para engañar a los usuarios de la banca y esta protección aunque las entidades financieras las tratan de detectar son modelos destinados a que sea el usuario quien debe ser cauteloso de estas tácticas.
Así por ejemplo podemos observar en la siguiente imagen un ejemplo de Phishing del Banco Santander:

Ilustración 3: Ejemplo de Phishing Banco Santander[39]

Estas pantallas redirigen a páginas parecidas en donde solicita el acceder con clave y usuario y de esta forma se entrega la información personal de la cuenta bancaria a los ciber delincuentes.

2.3.2 Ciberestafa

La estafa ya la habían identificado las antiguas civilizaciones, y así por ejemplo el Código de Hammurabi ya sancionaba la alteración de pesas y medidas, así mismo el Código de Manú establecía la tipificación de la venta de grano bueno por uno malo, o hierro por plata etc. Es un concepto que se lo utiliza a diario en nuestra vida cotidiana utilizando el término engaño.

[39] Oficina de Seguridad del Internauta (2019). *Ejemplo de Phishing Banco Santander.* Recurso Online, disponible en « https://www.osi.es/es/actualidad/avisos/2018/02/phishing-al-banco-santander » (última consulta 25 de agosto de 2019)

Lo primero que se nos viene a la cabeza cuando hablamos de este delito informático es el concepto típico de la estafa, en este vienen los elementos de engaño, error, acto de disposición patrimonial, perjuicio. En la estafa el bien jurídico a protegerse es el patrimonio, pero también es importante la buena fe y la confianza que se genera. Por esta razón no existe un listado o especificación de la variada gama de formas de realizar una estafa y con el ingenio de los delincuentes y tecnología pueden existir ilimitadas formas de cometerlo.

Según el Código Penal español en su artículo 248 dice que "1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno", pero además en el inicio dos letras a) se establece que también "Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo en perjuicio de otro" [40].

El segundo elemento nos habla claramente del concepto de ciber estafa, y es la actividad realizada por un medio informático. Al igual que la letra b) que señala que "Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

En la letra c) del mismo inciso nos detalla sobre una actividad especifica de los servicios bancario y detalla "Los que utilizando tarjetas de crédito o débito o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero" [41].

Así, también el Código Integral Penal del Ecuador en su artículo 186 señala que la estafa tiene una pena privativa de libertad de cinco a siete años, cuando se cometiere un fraude electrónico por medio de usos de tarjetas, o pagos. Y en la legislación intenta ser más específicos sobre las formas de alterar los dispositivos así señala por ejemplo la clonación, captura, alteración etc.

También nos habla sobre la persona que otorgue información falsa, induzca a la compra o venta pública de valores por medio de fraude, realice cotizaciones ficticias y cualquiera que se cometa por medio del Sistema Financiero Nacional será sancionado con la pena máxima de 7 años[42].

Como nos damos cuenta también el Código Integral del Ecuador existe una sanción para la comisión de la Ciberestafa y la hace con la especificación del uso de los dispositivos electrónicos.

[40] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
[41] Ibidem.
[42] Registro Oficial N.189, de 10 de febrero de 2014. Código Orgánico penal del Ecuador.

Este delito sigue siendo uno de los más prevalentes en el ciberespacio así por ejemplo el 12 de julio de 2019 se detienen 24 personas de una organización criminal internacional que utilizaban tarjetas vinculadas a los sistemas pago Wallet y NFC, según la noticia que ha dado el diario ABC de Madrid se defraudaban más de un millón de euros anuales, y estos a su vez los blanqueaban comprando criptomonedas[43].

Otro ejemplo es la detención de Lupin, que con solo 23 años realizaba un fraude de 300.000 euros al mes, este joven es considerado el mayor estafador online de la histórica, lo que hacían es crear web falsas y clonarlas, pero también nos dice el diario el Mundo "Lupin siempre estaba innovando y pensando en nuevas estafas, y así por ejemplo engañó a gente para venderle gasóleo de calefacción barato en invierno y aires acondicionados en verano, o montaba ofertas específicas para los días del Padre y de la Madre" [44].

2.3.3 Cracking, Hacking

El craqueo inicialmente se conoce como un procedimiento químico en el cual se ataca a las moléculas para descomponerlas crear un compuesto más simple, es por esto que en ámbito informático fue utilizado este termino porque es un ataque a los sistemas informáticos y software con el animo de causar un daño, haciendo pedazos, descomponiendo su sistema y así obtener información.

Las personas que realizan esta actividad se los conoce como crackers, que en la traducción literal significa rompedor. Estos están caracterizados por tener grandes conocimientos sobre ordenadores y redes. Lo que hacen estos individuos es borrar, modificar, dañar, desprogramar algún sistema, programa, documento, en donde por medio de romper con la seguridad de las compañías o también de obtener la información como las contraseñas bancarias.

Los ataques mas conocidos son los que se generan en las empresas de redes sociales, en que en un momento dejan de funcionar o tienen algún fallo porque alguien desprogramo la información. Pero a su vez los bancos tienen millones de ciberataques de crackers que intentan entrar a sus sistemas para obtener información o causar confusión en los usuarios o solo por dañar la imagen del banco.

Así, por ejemplo, Jonathan James fue condenado a prisión por delitos de crackeo, ya que el 2000 robó un software a la NASA, y también la información de miles tarjetas de crédito

[43] ABC Madrid (201)). *Nueva ciberestafa millonaria que afecta a más de 300 personas en España.* Recurso Online, disponible en: « https://www.abc.es/espana/madrid/abci-detienen-24-personas-ciberestafa-millonaria-mas-300-afectados-201907121217_noticia.html» (última consulta: 20 de agosto de 2019).
[44] El Mundo (2019). *Detenido Lupin, el leonés de 23 años considerado el mayor ciberestafador de la Historia*. Recurso Online, disponble en:
«https://www.elmundo.es/espana/2019/07/05/5d1e4d6f21efa0ce7e8b4672.html»
(última consulta: 20 de agosto de 2019).

o Kevin Mitcnick quien es más conocido como Condor sustrajo las bases de datos de COSMOS, introducirse en el Pentágono etc.

Pero al hablar de un sector tan sensible como el de los bancos, estos deben destinar millones de dólares anuales para protegerse de los miles de ataques diarios que tienen sus sistemas informáticos, ya que no solo esta en riesgo la información personal de los clientes, sino dinero que puede muy fácil perderse en el ciberespacio. Lo que más se conoce son los miles de usuarios que han sido victimas de los cracking de las tarjetas de crédito, pero existen una infinidad de modalidades que estos crackers utilizan para obtener un beneficio por sus habilidades informáticas.

Mientras que los Hackers conocidos también como los piratas informáticos, aunque son confundidos por los crackers, por tener un conocimiento informático amplio y poder acceder a los sistemas informáticos, estos no lo hacen con un carácter delictivo sino por diversión. Esto no quiere decir que los hackers estén en cumpliendo la ley ya que delinquen al entrar en sistemas de seguridad ajenos, pero lo que no hacen es causar destrucción.

Lo que nos dice David Pereira, CEO de Secpro, "es que un hacker normalmente ataca una estructura con autorización del dueño de la infraestructura, mientras que un cracker no tiene autorización en absoluto de nadie para hacer lo que hace y normalmente tiene motivos maliciosos, es decir, robarte información, secuestrarla para luego pedir rescate"[45].

Esta es la diferencia teórica que existe entre estos conceptos y en la actualidad son las propias entidades bancarias quienes contratan a los hackers para que busques las líneas de desprotección en los sistemas bancarios. O también son reconocidos con dinero al avisar sobre algún fallo en sus seguridades.

2.3.4 Vishing

Cuando pensamos en esta modalidad de delito es conocida por ser una variación del phishing new age, y proviene de las dos palabras phishing and voice, ya que se utiliza dos elementos para el cometimiento del delito que son el teléfono y el internet. Al igual que el phishing lo que hace es engañarnos para dar la información personal de nuestras cuentas bancarias.

El funcionamiento del Vishing funciona de la siguiente manera se envía un mensaje al teléfono informando de compras con la tarjeta de crédito y se nos asigna un número para reportar si esta transacción no es nuestra, al comunicarse con ese número de teléfono se

[45] El Comercio (2018). *¿Cuál es la diferencia entre un hacker y un cracker?* Recurso Online, disponible en: « https://elcomercio.pe/tecnologia/actualidad/diferencia-hacker-cracker-noticia-490674» (última consulta: 24 de agosto de 2019)

nos pide la información bancaria para cancelar la compra, pero lo que ha sucedido que se entrega la información a los criminales cibernéticos.

Aunque este es un delito muy nuevo existe una variedad y sin numero de elementos que crean la confusión en el usuario bancario es así como utilizan música del banco, voces de las entidades bancarias, envió de mensajes idénticos de números semejantes al de las entidades. Y los usuarios por la premura de solucionar el problema con sus tarjetas proporcionan toda la información.

2.3.5 Cross Pharming

Este también se lo conoce como una variación del phishing, también es el resultado de unir las dos palabras phishing y farming. Los criminales informáticos crean páginas idénticas de las entidades bancarias para que el cliente bancario al acceder a estas inserte su clave y su usuario, entregando involuntariamente la información de sus cuentas bancarias.

La perfección del diseño, copia tanto de la página web como del nombre de dominio de la entidad bancaria, lo que tiene de nuevo esta modalidad es que no hay equivocación el URL o el enlace, esto lo hace un hacker especializado que por medio de virus cambia el fichero host y lo redirige al usuario a la página que es creada de forma identidad a la de la entidad bancaria.

2.3.6 Fake Apps

El mundo del internet y de la banca cambio por completo con el aparecimiento de las apps, que son las aplicaciones móviles que a finales de los años 90 fueron creadas y que fueron desarrollándose con el pasar de los años.

Las entidades bancarias como una estrategia para ser parte de este cambio de forma de gestionar las cuentas bancarias por sus clientes, pone en funcionamiento aplicaciones que son parte de teléfonos electrónicos y de tablets. Aunque sin duda estas aplicaciones han mejorado la forma de gestión y brindado agilidad a la actividad bancaria. Estas también han sufrido grandes ataques y clonaciones.

Por lo que los criminales informáticos lograron entrar productos falsos a la cuenta de google play en donde los usuarios se bajaron estas Apps maliciosas y entregaron información de sus cuentas bancarias a los ciber delincuentes. Por ejemplo, en la India fueron tres bancos que sufrieron estas clonaciones en base a un incremento en la deuda crediticia.

Por ejemplo, aquí se muestran algunas imágenes de Fake Apps

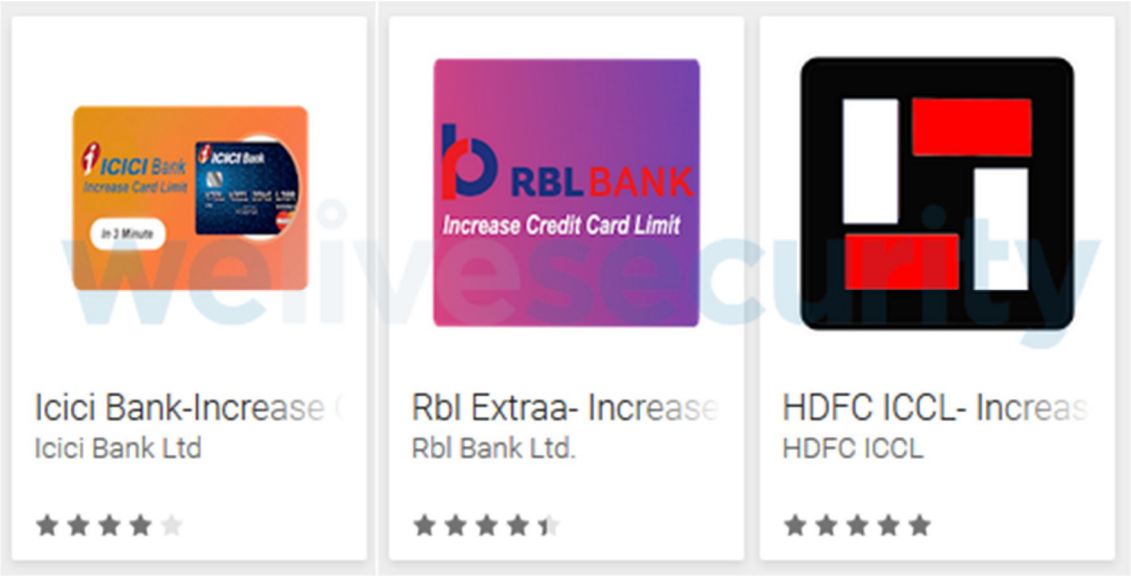

Ilustración 4: Ejemplos de aplicaciones falsas.[46]

2.3.7 Malware

Este es otra forma de cibercrimen, pero a diferencia de los otros que son ataques específicos a una entidad o un sistema, estos Malware se encuentran activos los 365 días del año y se esparcen sin control infectando al ciberespacio.

Malware es un Software malicioso, es cualquier programa, código, virus, aplicación, código informático que se utiliza para causar un daño en los sistemas de las entidades privadas y publicas y también a los pequeños usuarios que podrían ser infectados por medio del uso computadoras.

Sin duda hemos escuchado con mucha frecuencia el peligro que corremos al ser infectados por virus como Troyanos, Worm, Hijackers, Skyware y así existen un sinnúmero de versiones que han causado perjuicios en las redes sociales. Así por ejemplo en el 2018 el gusano Conficker ataco a 15 millones de servidores.

Esta información que corresponde al año 2017 señala que "Según la firma de seguridad informática, Kaspersky, a diario se crean poco más de un millón de diferentes tipos de malware, es decir que cada 12 segundo hay nuevo código malicioso que puede robar, destruir, encriptar o secuestrar millones de piezas de software de los diferentes sistemas operativos que existen hoy en día" [47].

---

[46] Espinal. J (2018). *Ejemplo de aplicaciones falsas*. Recurso Online, disponible en « https://www.downloadsource.es/como-identificar-app-falsas-o-fraudulentas-en-google-play-para-android/n/11736/» (última consulta 30 de agosto de 2019).

[47] Unocero. (2017). *Los malware más peligroso y devastadores en toda la historia*. Recurso Online, disponible en «https://www.unocero.com/noticias/los-malware-mas-peligrosos-y-devastadores-en-toda-la-historia/». (última consulta 30 de agosto de 2019).

Dentro de los Malware tenemos un sin numero de variantes es así como, por ejemplo:

Los Adware son aquellos que invaden con publicidad de productos o servicios.

Los Blackdoors su traducción es puerta trasera, en donde se crean accesos ocultos a los sistemas para poder ejecutarlos de formas maliciosas.

Los Botnet son computadores que han sido infectados con códigos maliciosos, estos trabajan en forma conjunta y distribuida difícil de detectarlos. Se los comparan con los zombis ya que trabajan sin que el usuario se de cuenta que es manipulado por un tercero.

Los Hoax son conocidos por la distribución de correos electrónicos con información falsa, hacen creer a los usuarios de algún evento o actividad es cierta. Estos mensajes son comunes en los sectores bancarios desestabilizando a las entidades por ejemplo con mensajes de una posible quiebra.

Los Keylogger lo que hacen este tipo de virus es archivar todo lo que el usuario inserte con su teclado y así obtener la información personal de claves y acceso a cuentas bancarias u otras entidades.

El Rogue es un software que esta básicamente su descripción es falsa, es decir que no hace para lo que fue creado. Así existen muchos programas que dicen optimizar la computadora, o ser antivirus, pero en realidad son lo contrario.

Los Spyware como su nombre lo señala es de espionaje, en este se recopila información para después vender la misma, chantajear, o publicarla. Pero a su vez son aquellas que detectan información de los IP y URLs así pueden crear parámetros de mercadotecnia en los usuarios.

Estos son algunos de las variaciones que existen de los malware y existen una infinidad de otros tipos que seria imposible describirlos, además que como se a mencionado se crean a diario millones para intentar infectar la red.

2.4 Que hace la banca para protegerse de los ciber criminales

Al verse rodeados de ciber ataques las entidades bancarias tienen normativa para protección de los usuarios y de la economía nacional y mundial. El Foro Económico Mundial los considera a estos ataques como uno de los tres principales riesgos de la economía mundial. Por esta razón las entidades bancarias y las regulaciones internas de los países como internacionales establecen manuales de seguridad que recogen las instrucciones, medios, mecanismos de protección ante ciberataques.

Estos manuales son distintos, pero deben tener los parámetros establecidos por la entidad bancaria, deberán ser cumplidos por todos los empleados bancarias y también la vigilancia del cumplimiento será cargo de los bancos que asignaran a personal que se

encargue del seguimiento de estos procedimientos. Las personas que estén a cargo de la misma deben tener la formación idónea y conocimiento para ejercer por ejemplo el cargo de director de seguridad de una institución bancaria.

Estas políticas han sido una prioridad en las entidades bancarias por el incremento de los ciberataques que han costado millones de dólares, en la actualidad se han conformado equipos de monitoreo ante los posibles riesgos informáticos, los correos electrónicos, llamadas, mensajes deben estar completamente autenticados las 24 horas del día los 365 días a la semana.

Además, de los mensajes de alerta sobre como un usuario debe protegerse son enviados como una política de seguridad, por ejemplo, hacen mención de no abrir correos sin verificar, no entregar claves, usar buscadores, no descargarse ficheros adjuntos entre otros. A su vez muchos bancos tienen campañas de comunicación alertando a los usuarios de las precauciones para no ser victimas de estos delitos.

También existen empresas especializadas que son contratadas para brindar la protección a los bancos, y de monitorear las posibles alertas de ataques de cibercriminales. Estas empresas también desarrollan software y sistemas que brincar más seguridad a los bancos y así puedan ir a la par del desarrollo tecnológico.

Pero adicional a estas políticas la banca española esta obligada a tener ciertos mecanismos de protección como un departamento de seguridad o un director de seguridad y esto se complemente con las Directrices que European Banking Authority que como ejemplo establece para todo el marco europeo por ejemplo sobre la seguridad de los pagos por internet (EBA/GL/2014/12), o las medidas de seguridad para los riesgos operativos y de seguridad asociados a los servicios de pago en virtud de la Directiva (UE) 2015/2366 (PSD2) etc.

O a su vez podemos tener algunas recomendaciones de la Comisión de las Comunidades Europeas, como por ejemplo e 8 de diciembre de 1987, sobre un Código europeo de buena conducta en materia de pago electrónico (Relaciones entre organismos financieros, comerciantes-prestadores de servicios y consumidores), Decisión marco del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, o la Decisión del Banco Central Europeo de 20 de abril de 2011, sobre la selección de proveedores del servicio de red de TARGERT2 (BCE/2011/5) etc.

Una de las más recientes es la directiva comunitaria PSD2 (Payment Service Directive 2) que entro en vigencia en enero de 2016 y su implementación no se podía exceder del primer o segundo trimestre de 2019, su principal objetivo es dar una mayor cobertura de seguridad y protegernos ante los fraudes en las operaciones bancarias, además del consentimiento del uso de datos que proporcionamos a la entidad bancaria. Una de las novedades que tiene esta directiva es que permite que los medios de pago sean realizados

por terceros sin necesidad de pasar por los bancos esto con el objetivo de dar más libertad al mercado, pero a su vez insertando una doble autentificación o hasta tres formas de acceso a las transacciones.

Aunque las formas de cometer delitos contra las entidades bancarias y los usuarios son cada día más creativas y agiles, también tanto las entidades gubernamentales nacionales como internaciones y los propios bancos destinan grandes cantidades de dinero para protegerse e innovar y así estar preparados para cualquier ataque.

CAPITULO 3

3. ANÁLISIS DE CASOS: SISTEMA DE SEGURIDAD EN LOS PRINCIPALES BANCOS ECUATORIANOS Y ESPAÑOLES

Es importante conocer cuales son los sistemas de seguridad que tienen los bancos, estos sistemas están destinados a brindar una protección ante los peligros externos que se nos puedan presentar en especial ante en el cometimiento de delitos.
Estos sistemas funcionan de forma interrelacionada y tienen desde indicadores de alarmas, transmisión de datos, logística y reacción de ataques etc.

En base a la Orden INT/317/2011, de 1 de febrero de 2011, sobre las medidas de seguridad privada, por normativa los bancos, cajas de ahorro y las demás entidades de crédito deben tener un departamento de seguridad. Para lo cual en este análisis revisaremos cuales son los sistemas de seguridad que los Bancos de España y Ecuador nos indican que están utilizando para brindar esta protección a sus usuarios.

Aunque al hablar del tema de seguridad consta de elementos referentes a especificaciones de sucursales, cámaras de seguridad etc., por nuestro tema de estudio nos centraremos al análisis de la seguridad online.

3.1 Sistema de seguridad en los principales bancos españoles

3.1.1 Banco Santander

El Banco Santander en su ingreso a su página web «www.bancosantander.es» se encuentra con un certificado valido que esta emitido por el DigiCert SHA Secure Server CA, esto nos garantiza que podemos estar seguros de que nos encontramos en una red segura. Utilizando el algoritmo de Encriptación RSA (1.2.840.113549.1.1.1), esta forma (Rivest, Shamir y Adleman esta basado en la factorización de números enteros). Además, nos señala que esta en uso 79 cookies.

Para ingresar a nuestro sistema del Banco Santander es decir la Banca Digital debemos indicar nuestro clave de acceso y firma electrónica, además de tener uno seguridad adicional que es la OTP (One Time Password), esta esta destinada a ser utilizada cuando se realicen transacciones adicionales. Por lo que se enviará una sola vez como mensaje de texto para alguna actividad en especifico considerada sensible.

En la página de información online el Banco Santander tiene una explicación de la seguridad online para lo cual nos establece que:

1. Monitoreo del Fraude. ". Para proteger tu dinero empleamos metodología de detección temprana de operaciones que pueden parecer fraudulentas"[48].
2. Extractos y justificantes online, aquí los canales de información están actualizados y abiertos para que los usuarios se percaten de movimientos que sean sospechosos.
3. Datos Cifrados.- El Banco Santander tiene cifrados y encriptadas sus datos para que mantengan su confidencialidad y solo el dueño de la información tenga acceso a ella.
4. Servicios de Antiphishing, antimalware y antitroyanos.- en este punto el Banco Santander señala que estos servicios se los ha destinado a empresas especializadas para la protección y vulneración del sistema.
5. Desconexión automática por inactividad.- es otra de las formas que tiene este Banco, que se debe iniciar de nuevo si se mantiene inactivo.
6. Protección de Sistemas. - El Banco tiene el uso de firewalls y antivirus con actualizaciones permanentes y esto acompañado de auditorias de seguridad.
7. Bloqueo de Claves. - También consta de cuando se tiene repetidamente incorrecta las claves se debe comunicar con el departamento de seguridad para el desbloqueo correspondiente.

Además, el Banco Santander tiene información para los usuarios de cómo protegerse ante los posibles ataques informáticos, en especial de el Phishing, Ransomware y nos da los parámetros de cómo debe ser nuestra contraseña, que consta de once dígitos y debe contener letras mayúsculas, números y símbolos. Además, nos da una herramienta que se llama Secure Password Check que esta destinada a ayudar a los usuarios a tener contraseñas más seguras.

Un elemento interesante sobre la seguridad online es que el Banco Santander tiene un Test de seguridad On-line para sus clientes y los califica de escaso, normal, avanzado, sobresaliente y experto. Así el Banco tiene un lema "De poco sirven todos nuestros sistemas de seguridad si tú no proteges tu mundo online." Por eso además de todos los controles y seguridades que tiene el banco, tiene una amplía gana de videos e información sobre como no caer en fraudes electrónicos [49].

Pero adicional tiene otros consejos como por ejemplo que hacer si te roban la tarjeta, o si existe una fuga de fatos, el control del ordenador parental, modos de mejorar la seguridad online, consejos de seguridad en la nube a la hora de trabajar, amenazas de seguridad móvil. Estos son solo algunos de los temas que tiene el banco, esto nos demuestra que ellos apuestan por la seguridad que deben tener los usuarios a la par de los que hace el banco.

[48] Santander. (2019). *Nuestro Compromiso con tu Seguridad*. Recurso Online, disponible en «Santandehttps://www.bancosantander.es/es/particulares/banca-online/seguridad-online/nuestro-compromiso-de-seguridad». (última consulta 30 de agosto de 2019)

[49] Ibidem.

También ha puesto al acceso de sus clientes un Trusteer Rapport, que es un programa de seguridad "detecta los posibles ataques eliminando automáticamente los virus o programas maliciosos de tu ordenador, manteniendo tu información y tus cuentas más protegidos" [50].

Este es un software gratuito, que se instala en los ordenadores de los usuarios de forma sencilla, esto brinda una protección adicional impidiendo la infección con programas maliciosos y los ataques de suplantación de identidad, protege las claves de acceso, las actualizaciones automáticas, antivirus etc.

Pero además de estas seguridades que podemos establecer, el Banco Santander hace público si existe algún intento de romper con la seguridad del Banco, es así como en su página web establece un aviso de ha existido un ataque ante la filial SIVASA de las tasaciones hipotecarias y puntualiza que ha sido avisado a la Policía.

Además, de las campañas que realizan conjuntamente la Policía Nacional para reforzar la seguridad en las medidas de pago y como no ser victima de los ciber crímenes, esta campaña se la realizó el 24 y 28 de junio de 2019. A su vez tienen videos prácticos de protección de contraseñas.

La información técnica del Banco sobre su seguridad la podemos resumir en lo siguiente primero la utilización de Equipo de Firewall, "valida el tipo de tráfico que entra y sale de los servidores y, a su vez, define un único punto de entrada en el cual se aplican controles adicionales de inspección y validación de paquetes de tráfico" [51].

Como segundo elemento el SSL que es un protocolo de comunicaciones (Secure Sockets Layer y HyperText Transport Protocol), este cifra todo el contenido generado en las comunicaciones así estas no puedan ser descifradas por terceros.

Desde hace unos años el uso de Cookies se encuentra presente en todas las páginas bancarias, esto ayuda al mejoramiento del uso del sitio de internet que accedemos. Lo que hacen las cookies es que son archivos de sitios de internet que contienen pequeñas cantidades de datos que mejoran el uso de los sistemas de una página de internet. Además, señala que otras medidas que tiene el Banco son so de codificación de campos en las bases de datos, auditorías internas y externas, el uso de software antivirus y sistemas de supervisión, entre otros [52].

---

[50] Santander. (2019). *Que es Trustter Rapport.* Recurso Online, disponible en «https://www.bancosantander.es/es/particulares/banca-online/seguridad-online/ibm-trusteer-rapport.» (última consulta 30 de agosto de 2019).

[51] Santander. (2019). *Seguridad del Sistema.* Recurso Online, disponible en «https://www.pb-santander.com/es/confidencialidad/seguridad-del-sistema» (última consulta 30 de agosto de 2019).

[52] Santander. (2019). *Seguridad del Sistema.* Recurso Online, disponible en «https://www.pb-santander.com/es/confidencialidad/seguridad-del-sistema» (última consulta 30 de agosto de 2019).

3.1.2 Banco Bilbao Vizcaya Argentaria BBVA

Cuando hablamos de cuales son los sistemas se seguridad que utiliza el BBVA debemos comenzar por su página de internet, la dirección es «www.bbva.es» y que podemos verificar que cuenta con un certificado valido que es otorgado por la empresa DigitalCert Inc. de Estados Unidos de América. Y además inmediatamente nos aparece las cookies informando que al aceptarlas nos ayudaran en la experiencia de navegación.

BBVA aclara que tres buscadores son efectivos para usar su página web y son Internet Explorer en la actualidad Microsoft Edge, Firefox, Chrome en su página web. Hasta especifican en la página web es la optimización de la resolución de pantalla y que se encuentran funcionando 134 cookies, para que los usuarios tengan una mejor visualización y esta consta de 1280 X 800 píxeles.

Al igual que el Banco Santander estos utilizan el protocolo SSL (Secure Socket Layer), "El servidor seguro transmite la información cifrada mediante algoritmos de 128 bits, que aseguran que solo sea inteligible para el ordenador del cliente y el servidor del banco" [53]. Como lo habíamos mencionado esto da una protección a los usuarios para que la información del sistema no sea usada por terceras personas y que sus claves tanto de las tarjetas PIN como de clave de acceso se encuentren cifradas.

Pero existe algo que diferencia al sistema del Banco Santander que este Banco tiene el sello de la Asociación Electrónica (ACE), Asociación de Certificación Electrónica (ACE), nos avala como la primera entidad financiera adherida a su Código Ético de Protección de Datos en Internet [54].

También otro de los servicios que consta de la seguridad BBVA Net Cash que es un sistema que le permite al usuario elegir distintas formas de firma, estas pueden ser mediante clave de operaciones, que debe constar de 9 caracteres, firma por formula aritmética por un número indicado, esto da una seguridad adicional a los clientes.

El sistema de BBVA consta de un doble factor de seguridad que es el Token Plus para la validación para la validación en el circuito de usuarios y la firma de operaciones a través de BBVA net cash. "De esta forma y con este fin, el sistema le solicitará que introduzca el código de seguridad de seis dígitos generado por Token Plus (de uso único) además de su clave de firma. El dispositivo es personal e intransferible, se entrega uno por usuario firmante" [55].

---

[53] BBVA, (2019). *Seguridad*. Recurso Online, disponible en «https://www.bbva.es/sistema/meta/seguridad/index.jsp» (última consulta 30 de agosto de 2019).
[54] Idem.
[55] BBVA, (2019). *Seguridad en BBVA net Cash,* Recurso Online, disponible en «https://demo.bbvanetcash.com/SESKYHP/seguridad_es.pdf» (última consulta 30 de agosto de 2019).

Una cosa importante que a puesto en el documento de su página web el Banco BBVA, da también de las características físicas de los procesadores de datos así indica CPD bunkerizado, y los Centros de Datos plenamente operativos las 24 horas del día.

Adicional que al igual que el Banco Santander tienen en su página web brinda información al usuario de cómo prevenir y tomar precauciones antes los criminales informáticos. Dando consejos como el tener siempre copias de seguridad, o tener antivirus activos, verificar los sitios seguros de internet etc.

3.1.3 Caixa Bank

Cuando entramos a Caixa Bank su cuenta «www.caixabank.s», podemos verificar que cuenta con un certificado valido emitido por la empresa Digital Media Services Inc. Y que al ingresar al sistema estamos utializando de 134 cookies, que mejoran el funcionamiento de esta página.

Existe una caracteristica importante que tiene este banco y que ofrece un servicio denominado CaixaBankProtect, en el cual señala que con esto los usuarios estan protegidos ante cualquier fraude y sin costo. Siempre que estas compras hayan sido el día que ha sido bloqueada por perdida, falsificación y los trece meses anteriores a esta. Esto es un plus en la protección que da a los clientes.

También tiene un servicio de CaixaBank Sing que es la firma digital que pemite la autorización de tus transaciones y operaciones con la máxima seguridad y todo esto se lo realiza por el telefono movil, este banco tiene una apuesta por la inmovacción y el uso de la banca movil.

También este Banco tiene desde el 2017 la identificación por Face ID que se implementa en el Iphone X, por lo que desde la banca movil podran racceder a través del reconocimiento facial a sus cuentas. Pero no es esta la unica innovación e implementación de seguridad, otra que podemos señalar es los sistemas contactless de pago por el movil.

Igualmente, algo que ha lanzado este banco es el reconocimiento facial de los cajeros automaticos y así lo dio a conocer Gonzalo Gortázar delegado de este banco el 14 de febrero de este año. Con la implementación de seguridad además de agilizar el proceso, brinda una mayor seguridad. Debemos mencionar que esto se hizo por medio de dos empresas de tecnología Fujitsu y FacePhi. Esto ha hecho que caiza el primer banco que brinda la tecnología biometrica.

Y no podemos olvidarnos de una de estos ficheros que la tienen en la actualidad todos los sistemas informaticos conocidos como las cookies de navegación, como muestra la ilustración que esta a continuación.

Ilustración 5: Enunciado de aceptación de cookies CaixaBank[56]

Las garantias técnicas de seguridad son "cifrado se basa en el protocolo estándar SSL-V.3 y utiliza claves criptográficas de sesión de 128 bits de longitud." además de la linea abierta que tiene el cliente y los sistemas informáticos de cifrado [57].

Al igual que los otros bancos intenta concienciar a los usuarios de su sistema a protegerse ante los posibles ataques y criminales, para lo cual establece las 10 reglas de navegación segura que entre las más importante podemos señalar la utilización de antimalware actualizado, las actualizaciones de los sistemas operativos, la utilización de contraseñas robustas, no acceso de sitios de dudosa reputación, tener cuidado con resdes wifi gratuitas etc.

3.1.4 Bankia

Al ingresar a la página web de Bankia que es «www.bankia.es »podemos visualizar que tiene un certificado valido otorgado por DigiCert Inc., lo que no nos ha solicitado esta página web es la aceptación de las cookies, pero se encuentran funcionando 47 de ellas.

La información del manejo de la seguridad en esta entidad bancaria nos menciona tres líneas que la primera es el monitoreo de los sistemas y redes, monitorización del fraude y test periódicos de intrusión.

La Banka Online de Banka menciona solamente que se puede acceder por medio de la clave de acceso y el código de verificación de algunas transacciones consideradas sensibles por medio de un mensaje de texto y de la firma electrónica.

---

[56] CaixaBank (2019). *Enunciado de aceptación de cookies CaixaBank,cai* Recurso Online, disponible en « https://www.caixabank.es/particular/home/particulares_es.html » (última consulta 30 de agosto de 2019).
[56] BBVA, (2019). *Seguridad en BBVA net Cash,* Recurso Online, disponible en «https://demo.bbvanetcash.com/SESKYHP/seguridad_es.pdf» (última consulta 30 de agosto de 2019).
[57] Caixabank (2019) *Aspectos importantes de seguridad Aspectos legales*. *CaixaBank.* Recurso Online, disponible en «https://www.caixabank.es/particular/seguridad/seguridadlacaixa_es.html#garantias_tecnicas» (última consulta 30 de agosto de 2019)

Este banco tiene campañas sobre la seguridad a sus usuarios por medio de videos dinámicos, que muestra las formas que los usuarios se pueden proteger ante posibles ataques bancarios.

3.2 Sistema de seguridad en los principales bancos ecuatorianos

3.2.1 Banco del Pichincha

Este Banco al ingresar a su página web «www.bancodelpichincha.com» nos solicita la aceptación de las cookies y además en uso se nos informa que están 73. Podemos verificar que cuenta con un certificado valido otorgado por DigiCert Inc. que es una empresa de Estados Unidos.

Los usuarios del Banco del Pichincha tienen sus claves utilizando el cifrado SSL a 128 Bits y consta de un certificado emitido por Verising que es una empresa que soporta la infraestructura de red. Nos hace una aclaración sobre el funcionamiento de este cifrado en su web diciendo que solo la sección de clave y usuario y la información financiera se utiliza, mientras que la otra información para un procesamiento más rápido.

Este Banco sus formas de seguridad con las claves de usuario, contraseña y el PIN telefónico, este último utilizado para la confirmación para algunas de las transacciones electrónicas. Además, se solicita una clave de doce caracteres que deberá tener combinación entre letras y números. Adicional tiene la selección de una figura como un segundo elemento de entrada al sistema.

Y esta se entrelaza por medio de un servicio de alertas que cualquier movimiento que se haga llegara la información al mail o al teléfono celular, ya sean transferencias o retiro en efectivo. Además de la aplicación que tiene se utiliza el reconocimiento facial para acceso de esta.

Al igual que otros bancos tiene información para los usuarios sobre formas de cuidar la seguridad, como el no compartir las claves, no realizar compras de quienes no se conoce, tener siempre actualizado el software y acceder a antivirus.

Este Banco tiene una línea de urgencias bancarias las 24 horas a las cuales se puede acceder si es que verificamos algún movimiento de nuestras cuentas o si queremos hacer cancelación de tarjetas etc. Esto se debe a que la forma de desarrollarse el sistema bancario en el Ecuador es diferente a la modernización y uso de redes de países como los europeos.

3.2.2 Banco del Pacifico

Al ingresar al sistema del Banco del Pacifico no existe una aceptación de ninguna cookie para el mejoramiento de la página, pero en uso consta 37 cookies. La página es

«www.bancodelpacifico.com» que consta de un certificado valido otorgado por la empresa DigiCert Inc.

Este banco para el ingreso a su sistema consta de claves dinámicas (OTP) "los códigos OTP (siglas del término inglés One Time Password) son códigos numéricos de un solo uso que se utilizan para una sola transacción. Los recibirás a través de un SMS en tu teléfono móvil cada vez que quieras ejecutar cualquier operación o realizar cualquier petición a través de tu banca a distancia" [58].

En esta Banca Virtual esta cifrado y como medida de seguridad tienen un agente virtual sophie para cualquier ayuda y consulta y adicional es que la Banca Móvil tiene el reconocimiento fácil para ingresar al sistema.

También tiene algunos canales de información sobre los fraudes informáticos, pero es bastante escaso la información sobre su sistema y las formas de protección del usuario ante un ciber-crimen, ya que en especial hablan del phishing, pero no hacen mención de las otras formas de fraude.

3.2.3 Banco de Guayaquil

Cuando ingresamos al sistema de este banco, tampoco se nos ha solicitado adherirnos alguna cookie del sistema, pero consta de 57 cookies en uso. La página del Banco es «www.bancoguayaquil.com» que cuenta con su certificado valido otorgado por la empresa GlobalSign nv-sa.

Este banco si detalla más sobre las medidas de seguridad que tiene una de ellas es el uso de la tecnología SSL (Secure Socket Layers), que es quien nos confirma el cifrado de la información. Esto esta acompañado de las seguridades del usuario y contraseña que nos recomiendan si la contraseña es muy débil y podría tener riesgo de fraudes.

Otro servicio que presenta este Banco es One Time Password, que es el envió de un número por SMS que expira en un determinas minutos, y es utilizado para las transacciones consideradas más sensibles como por ejemplo la transferencia de dinero. Acompañado de las coordenadas que es una tarjeta con códigos entregada que deberá ser utilizada en cualquier movimiento de dinero.

Este Banco automáticamente asigna la desconexión en su sistema en un periodo de tiempo de inactividad, y se deberá ingresar de nuevo. Así se evita conexiones abiertas o algún tipo de fraude.

[58] Pibank. (2019) *¿Que es y como funciona el código OTP?* (2019). Recurso Online, disponible en «https://www.pibank.es/faq/que-es-y-como-funciona-cogido-otp/ »(última consulta 30 de agosto de 2019)

También el Banco de Guayaquil tiene información para sus usuarios de los peligros y desarrolla algunas advertencias antes el peligro de los gusanos de la web, del robo de identidad, o de los espías de la red, tratando que sus usuarios sean precavidos para no sufrir estos fraudes bancarios.

3.2.4 Produbanco - Grupo Proamerica

Al ingresar al sistema del Banco Produbanco no se encuentra ninguna solicitud de Cookies, pero al entrar a su sistema nos informa que están 51 cookies en uso. Además consta en su página web «www.produbanco.com.ec» el certificado del banco emitido valido por GlobalSign nv-sa.

El banco maneja su sistema con un sistema de encriptación de la información y también de acceso por usuario y contraseña a su sistema. Las claves y usuario del sistema se utilizan por medio de la validación del OTP, además de imágenes de identificación para el ingreso. Un paso adicional que puede solicitar este banco es la Pregunta Desafío que son tres preguntas personales para ser contestadas al ingresar al sistema.

Un paso importante que tiene este sistema es el Token digital, que es un dispositivo de seguridad que proporciona un código distinto, aleatorio, que vence con cada transacción. Esto se da por medio de una aplicación móvil que deberá ser usada en el teléfono celular.

Esta es la información que nos proporciona el banco de las formas que ellos protegen a es bastante escasa, no existe una información real de los mecanismos y del cumplimiento de normas de seguridad.

3.3 **Principal diferencia entre la seguridad de los sistemas electrónicos bancarios de Ecuador y España.**

Para entender a breves rasgos sobre la seguridad bancaria que tiene Ecuador y España, las diferencias que me he percatado en la búsqueda de información se debe comprender que los bancos no nos van a compartir la información técnica de cuales son los mecanismos de protección a sus sistemas. Pero si nos hablan en breves rasgos cuales son los sistemas de protección que tienen relación con el usuario bancario, es decir con la entrega de claves o los accesos a su banca online y banca móvil.

Para dar una perspectiva general y entender cual es la principal diferencia entre estos dos países hacemos referencia al Estudio del Estado de la Ciberseguridad en el Sector Bancario de América Latina y el Caribe de la OEA La Organización de Estados Americanos, y es impresionante que señala que el “49% de las entidades bancarias aún no están implementando herramientas, controles o procesos usando Tecnologías Digitales Emergentes, tales como Big Data, Machine Learning o Inteligencia Artificial, las cuales

resultan muy importantes a la hora de prevenir ciberataques o determinar patrones sospechosos asociados a fraude, entre otras capacidades de detección"[59].

También este informe nos señala que 92% de las entidades bancarias presentan ataques informáticos y solo el 41% esta llevando acciones para la protección de los ataques cibernéticos. Pero el factor más importante que nos daremos cuenta es que se invierte el presupuesto del 43% en Plataformas y medios tecnológicos, un 22% en Recursos Humanos, un 22% en servicios tercerizados y un 13% en Generación de capacidades.

Como vemos el interés de la banca en Latinoamérica en la transformación tecnológica no es su principal objetivo, puesto que prima la seguridad física de las instituciones bancarias por la situación de inseguridad que se vive en estos países. En Ecuador aun existe el uso del papel moneda sobre los pagos electrónicos ya sea por transferencias bancarias o pago por tarjeta, es por esto que las instituciones bancarias destinan su presupuesto en entidades físicas que constan de seguridad y de mucho personal para deposito y retiro de dinero y otras transacciones bancarias.

Por esta razón la principal diferencia que puedo verificar en relación con los sistemas de seguridad electrónica de los bancos que hemos analizado de España como de Ecuador es que a nivel europeo el desarrollo de la seguridad bancaria electrónica es muy desarrollada, la información y medios de protección son puestos al alcance de los usuarios. Dan detalles de las plataformas, sistemas dando a los usuarios una real sensación de seguridad. Además de las múltiples campañas contra los posibles fraudes.

Al revisar los bancos ecuatorianos la información es escasa y se centran en el delito del phishing, pero con explicaciones muy sencillas de protección. Además, la información técnica, aunque en general los bancos se reservan y nos dan información especifica, en las entidades españolas las aglomeran para demostrar que se puede confiar en la entidad. Mientras que en las entidades ecuatorianas señalan que tienen los mejores sistemas de seguridad, pero sin especificar cuales son.

Para comprender mejor, este 14 de septiembre 2019 es obligatorio que la banca española aplique la doble autentificación para acceder a la banca online, y además como principal requisito el uso del móvil para acceder a la banca digital según la normativa PSD2 (Payment Service Directive). Mientras que en Ecuador sería impensable que sea obligatorio el uso del celular ya que existe un alto número de población que no cuenta

[59] OEA, (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.* Canadá. Recurso Online, disponible en « https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf» (última consulta 01 de septiembre de 2019)

con un teléfono celular inteligente, así solo tres de cada diez personas en Ecuador tiene acceso a Smartphone [60].

Las diferencias en los canales de acceso varían de banco a banco, pero si existe una modernización como en la implementación de los sistemas de reconocimiento facial y canales biométricos en cajeros automáticos que ya cuenta un banco en España y que aun no se encuentra accesible en Ecuador. A diferencia de las aplicaciones de la banca móvil que existe el reconocimiento fácil en los dos países.

Aunque pensaría que existirían otros factores comparativos, después de revisarlos podemos concluir que el sistema tecnológico de los bancos aun se encuentra poco desarrollado al igual que su seguridad en el Ecuador es por la forma en que se genera la economía al tener el uso de papel moneda como primera fuente de pago. Mientras que en España cuenta con sistemas inteligentes de seguridad, información y en especial de pago electrónico por esta razón pone mayor énfasis en la prevención de los ataques tecnológicos bancarios por que la relación banca cliente se desarrolla en un 80% por los canales virtuales de las instituciones bancarias.

[60] El Universo, (2018), *Tres de cada diez personas cuentan con smartphone en Ecuador*. Recurso Online, disponible en « https://www.eluniverso.com/noticias/2018/08/06/nota/6893255/tres-cada-diez-personas-cuentan-smartphone» (última consulta 01 de septiembre de 2019)

CAPITULO 4

4.1 EL LÍMITE DE LA SEGURIDAD ELECTRÓNICA BANCARIA

4.1.1 El limite de la responsabilidad civil de las Entidades Bancarias

Para comenzar el análisis de hasta donde llega el límite de la responsabilidad civil de las entidades bancarias, debemos precisar que la actividad bancaria es dinámica con una diversidad de funciones. Que la Banca además de tener una relación banca- Estado su principal relación es la banca - cliente por ende tiene una responsabilidad civil proveniente de sus contratos y obligaciones civiles, comerciales y financieras.

Además, que los bancos son entidades publicas y privadas y en su mayoría estas ultimas son de carácter comercial que realizan una actividad profesional de interés público y por ende están controladas por entidades estatales que determinan normas para su funcionamiento, lineamientos, limites.

Por esta razón las instituciones financieras y sus actividades bancarias se rigen por el ámbito del Derecho civil, por medio de la principal fuente de las obligaciones que es el contrato y este tiene una especificación que es contrato bancario que también tiene unas normativas y modelos de normativa nacional y supranacional. Pero con el cambio tecnológico también en la actualidad como usuarios debemos suscribir contratos como los de banca electrónica.

Para entender de una manera más amplia podríamos establecer que por medio del contrato bancario la institución bancaria queda comprometida su responsabilidad por la comisión de faltas dañosas, que estas acarrean una responsabilidad tanto civil como penal. Estos contratos bancarios hacen responsables a la banca a sus clientes, tanto en el hacer como no hacer de las obligaciones de estos contratos cuando su actividad les cause perjuicios.

Debemos precisar que estos contratos son de adhesión es decir que no son negociados individualmente, sino que los usuarios solo tienen la opción de aceptarlo o rechazarlo. Estos contratos cumples con los requisitos y formalidades de la Ley de Condiciones Generales de la Contratación (Ley 7/1998, de 13 de abril) y las normas especificas que tiene la actividad bancaria

El banco tiene la función de comisión mercantil, que o de mandato según el Código Civil Español en su artículo 1709 señala que “Por el contrato de mandato se obliga una persona a prestar algún servicio o hacer alguna cosa, por cuenta o encargo de otra.” [61] .

[61] Real Decreto de 24 de Julio de 1889 por el que se publica el Código Civil.

El Código de Comercio Español en su artículo 244 señala que " Se reputará comisión mercantil el mandato, cuando tenga por objeto un acto u operación de comercio y sea comerciante o agente mediador del comercio el comitente o el comisionista." [62]

Es por eso que la responsabilidad civil que se le otorga a la entidad bancaria es de profesional por la actividad que realiza, por las operaciones que se encuentran a su cargo por lo establecido en el código civil y en por el hecho de ser una sociedad al Capitulo II de las personas jurídicas y responden contractualmente por el incumplimiento frente a los usuarios bancarios.

Además los tribunales y la jurisprudencia del Supremo también ha establecido una protección a la parte más vulnerable en esta relación banca cliente, puesto que se considera que el banco tiene una infraestructura que esta precautelando que las seguridades no sean vulneradas ante un usuario que escasamente conoce sobre la protección y que no podría protegerse ante casos como clonación de tarjetas de crédito o ciber- crímenes, ya que ellos cumplen con el uso idóneo de la información que se encuentra a su disposición.

Estas actividades profesionales bancarias en la actualidad están incluidas las actividades normales y como parte de los servicios de los bancos, estas han cambiado ya que ahora no solamente se realiza deposito dinerario, emisión de cheques, cajas de seguridad, custodia de títulos valores, estas actividades siguen estando presentes en la banca pero la forma que se las realiza es completamente distinta, es aquí que la entidad tiene otra responsabilidad en sus actividades profesionales y esta ligada a todos los servicios que brinda a través de los medios tecnológicos.

Antes de entrar directamente a hablar de la responsabilidad civil de los bancos en los temas relacionados con los servicios electrónicos, debemos considerar que existen fallos por parte de las Cortes Españolas sobre la responsabilidad de cheques falsificados, dándole la responsabilidad al Banco con carácter profesional y establece que es parte del riesgo que tiene por la actividad que realiza.

Por esta razón podemos indicar que al ser parte de la actividad profesional el uso de los canales electrónicos, utilización de tarjetas de crédito los bancos deben asumir los daños que ocasionen estos riesgos que se utilizan y que ellos han puesto a disposición de los clientes y que en muchos casos estos servicios tienen una tasa remunerativa, como por ejemplo sacar dinero o realizar una transferencia bancaria.

Es así como en estos casos la prueba que debe presentar el banco va contra el usuario bancario señalando las razones de la producción del hecho, y la prueba sobre el cumplimiento de las seguridades electrónicas no exonera de la responsabilidad al Banco.

[62] Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio.

Entonces la pregunta que debemos hacernos cuales son las funciones que tiene la banca, ya que estas funciones fueron incrementando con el uso de la tecnología, pero sigue siendo su principal función el deposito de dinero y por ende la banca tiene la obligación de la custodia y manejo de la cosa depositada

El artículo 306 del Código de Comercio Español en su párrafo segundo señala que "En la conservación del depósito responderá el depositario de los menoscabos, daños y perjuicios que las cosas depositadas sufrieren por su malicia o negligencia y también de los que provengan de la naturaleza o vicio de las cosas, si en estos casos no hizo por su parte lo necesario para evitarlos o remediarlos dando aviso de ellos además al depositante inmediatamente que se manifestaren" [63].

Esta función en específico se encuentra avalada en el contrato que eran los conocidos como contratos de apertura de cuenta bancaria y ahora que también se suman los contratos de banca electrónica, debemos mencionar que ahora todos los actos jurídicos electrónicos se encuentran válidamente reconocidos esto así lo establece el artículo 23 numeral 1 de la Ley de Comercio Electrónico.

Y estos servicios de pagos que se dan por medio de la vía electrónica como la transferencia de dinero, operaciones de pago, líneas de crédito, pagos de tarjeta, envió de dinero etc. Deben ser autentificados por el banco y que estas se realizaron de manera correcta y el banco deberá probar que se registro y autentico. Cuando hablamos de autenticación es que el usuario bancario aceptado y aprobado esta operación.

Ahora en estos contratos electrónicos en las obligaciones que tiene el cliente bancario esta de la custodia del usuario, contraseña, del tótem y otra información que trata de garantizar el uso de estos servicios de manera efectiva, pero además el uso de esta información representa en los contratos bancarios una declaración de la voluntad de las actividades que se están desarrollando en los sistemas electrónicos. Además de informar al banco de las operaciones que se han ejecutado incorrectamente inmediatamente después de conocerlas.

Y las obligaciones que tiene el banco es la custodia y verificación de todo su sistema electrónico y también de las encriptaciones de la información que esta custodiando el banco, ya que no solamente ahora es una custodia del dinero sino también de la información personal, claves, nombres, movimientos bancarios etc.

Por esta razón existen algunas jurisprudencias civiles como La Sentencia núm.151/2013, de 7 de marzo de 2013 de la Sección 14ª de la Audiencia Provincial de Barcelona (Recurso de apelación 150/2012, PROV 2013\171665)., a Sentencia núm.429/2016, de 10 de noviembre de 2016, de la Sección 3ª de la Audiencia Provincial

[63] Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio.

de Vizcaya (Recurso de apelación 386/2016, AC 2016\2241), esta ultima estima la demanda por la falta de interposición de medidas de seguridad para así evitar el cometimiento del pishing.

En esta se realizan análisis sobre cuales son los medios técnicos que debería ofrecer los bancos ante los ataques de cibercrimenes y que estos se encuentran establecidos como parte de el servicio de los contratos electrónicos, aun así los medios de protección que debe desarrollar el banco son parte de su actividad profesional.

Cuando hablamos sobre el limite de responsabilidad que tiene el banco nos damos cuenta en que como hemos analizado la responsabilidad sobre el cometimiento de estos fraudes electrónicos termina siendo exclusivamente de la entidad financiera. Y como habíamos mencionado aun en el caso que este haya cumplido todas las normas de protección y seguridad electrónica bancaria no los deslinda de su responsabilidad.

Este análisis nos permite evidenciar que existe de alguna forma una desprotección a la entidad bancaria y que debe asumir la responsabilidad civil ante los perjuicios de los clientes por estos ciber delitos, dando una protección a los usuarios y también la responsabilidad del banco de ofrecer productos y servicios según el perfil del cliente.

Esto acarrea que además de todos los servicios que brinda la banca también deban no solo dar la información a los clientes sino que tanto productos como servicios sean entendidos y no un mero conocimiento de estos. Es por esto que a los bancos tienen campañas de educación de sus usuarios y les ha tocado brindar información al cliente, de los riesgos, de los delitos, de las formas de estar protegidos.

4.2 El límite de la responsabilidad de los usuarios bancarios

Cuando hablamos de la responsabilidad que tienen los usuarios bancarios debemos primero hacer referencia a cuáles son las obligaciones para el cliente al contratar un producto bancario, como estos son diversos estas obligaciones las establecen los contratos marco y también el Banco de España.

Así por ejemplo Orden EHA/1608/2010, de 14 de junio, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago. O Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios. (BOE de 29) (Corrección de errores BOE de 3 de diciembre), en esta dos ordenes tenemos algunas obligaciones que deben cumplir los clientes bancarios.

Así por ejemplo la obligación que tiene el cliente bancario de entregar información verídica a la entidad bancaria, informar a la entidad bancaria sobre algún movimiento sospechoso en sus cuentas, ser responsable en la custodia de usuario y pin de sus tarjetas y cuentas bancarias.

Sin duda el limite del cliente se basa en que esta custodia de las claves para acceso a los sistemas de banca online y móvil así por ejemplo sería muy fácil mostrar ante un juez que la persona expuso su seguridad bancaria al publicar una clave, o hacer un video donde se permite ver sus contraseñas para ingresar al sistema. El uso de la información y custodia de tarjetas de crédito de forma publica también puede ser ese limite que los legisladores muestren que un cliente actuó de manera negligente y no cumplió con esta obligación.

4.3 El riesgo estadístico: la necesidad del seguro bancario

Cuando nos centramos sobre cual es la posibilidad de que nos ocurra un fraude bancario, podemos nombrar algunos datos que nos darán la perspectiva de lo que se vive a nivel mundial y la necesidad de protección que deben desarrollar los bancos a cada segundo por estos riesgos.

A continuación, para dimensionar a lo que estamos expuestos he realizado una captura de pantalla del mapa en tiempo real de los ataques cibernéticos, en este establece que España se encuentra en el puesto 11 y en los primeros puestos tenemos Rusia, China, Alemania y Estados Unidos. Esta información la otorga en base algunos antivirus que detectan las amenazas, así como On Access Scan, On Demand Scanner, Mail Anti-Virus, Kas Kaspersky entre otros.

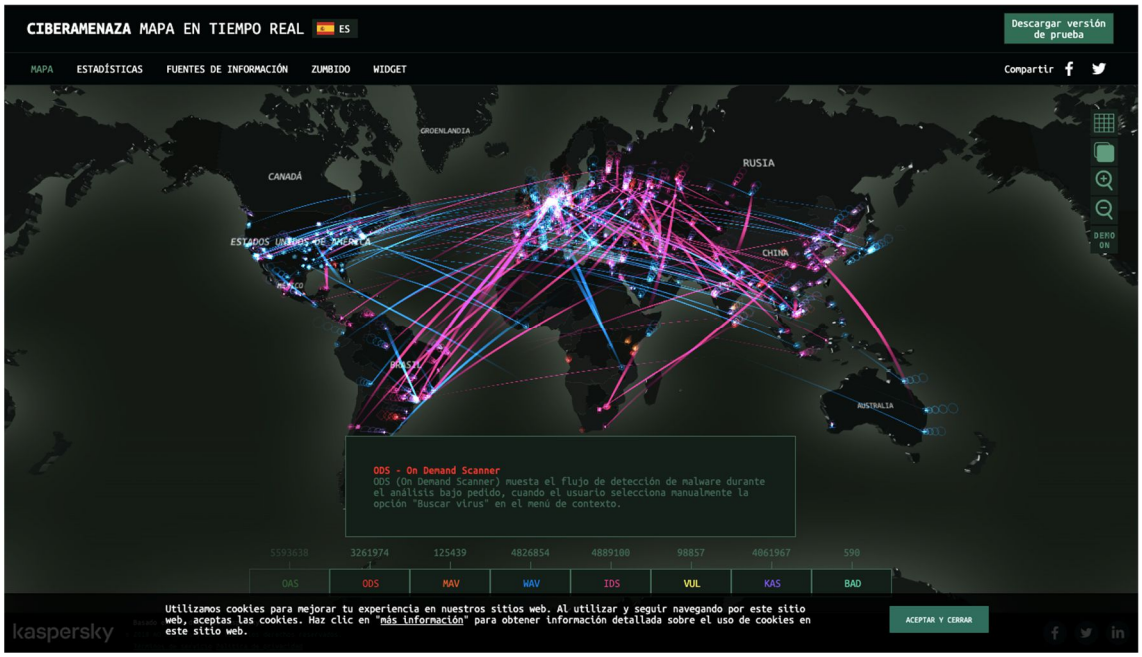

Ilustración 6: *Mapa en tiempo real de Amenazas Cibernéticas (Kaspersky)*[64]

[64] Kaspersky (2019), *Mapa en tiempo real de amenazas Cibertnéticas.*. Recurso Online, disponible en « https://cybermap.kaspersky.com/es» (última consulta 01 de septiembre de 2019)

En este mapa establece no solo de forma grafica como se ven los ciberataques en tiempo real, también va realizando un análisis por día y mes de los ataques que ha sufrido los diversos países.

Los países que estamos estado analizando son Ecuador y España y aquí les traemos un gráfico el cual muestra las infecciones locales del ultimo mes y también el porcentaje del tipo de virus que han sido infectados los sistemas de estos dos países.

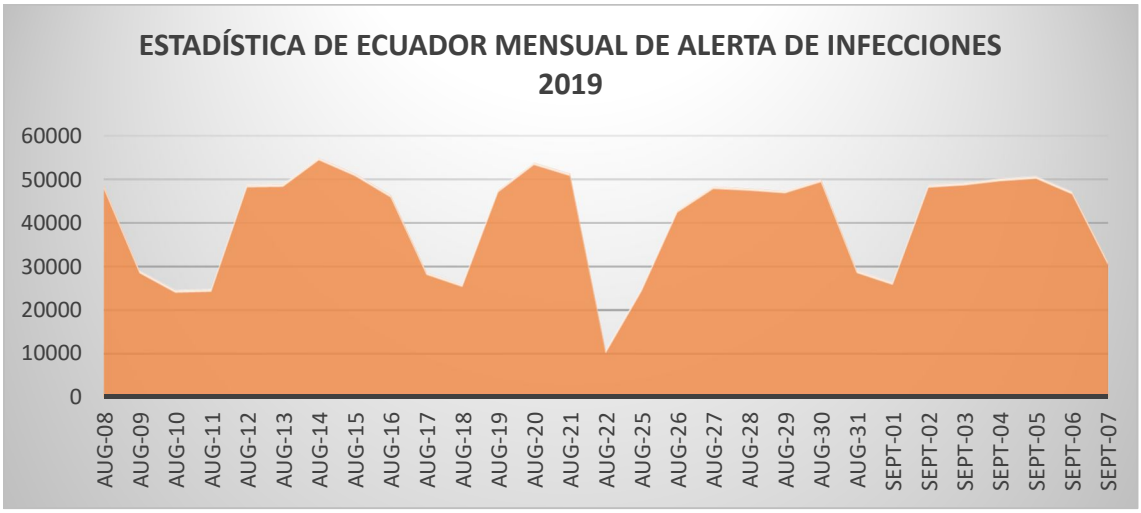

Ilustración 7: Estadística de Ecuador mensual de Alerta de Infecciones 2019[65]

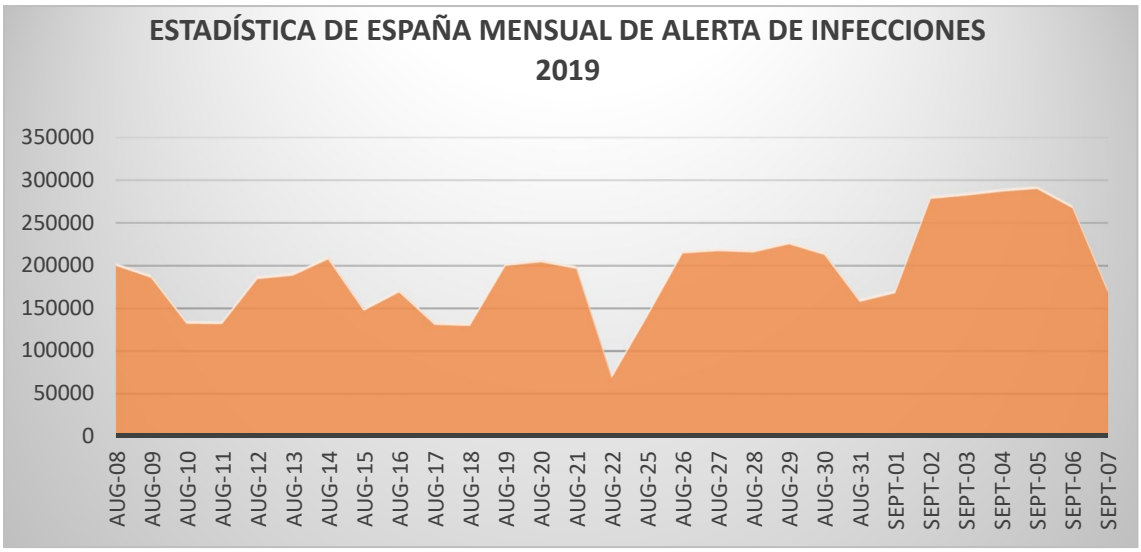

Ilustración 8: Estadística de España mensual de alerta de infecciones 2019[66]

[65] Kaspersky (2019), *Estadísticas de Ecuador mensual de alerta de infecciones.* Recurso Online, disponible en « https://cybermap.kaspersky.com/es/stats/» (última consulta 07 de septiembre de 2019)
[66] Ibídem.

Lo que nos demuestran estos cuadros estadísticos es que en España entre estos primeros días del mes existió un tope de ciberataques que se dieron el 3 Y 4 de septiembre de 2019 con 280975 y 289403 y el más bajo el 22 de agosto de 2019 con 71286 ataques.

A su vez el Ecuador tiene su mayor infección igual en el mes de septiembre en especial el 4 y 5 con 50130 y 50706 respectivamente y el menor el 22 de agosto de 2019 con 10659, al parecer en este ultimo existe una coincidencia.

Además, tenemos dos cuadros con información de Kaspersky Theast, que nos muestra en España cual ha sido el virus más utilizado con un 11.4% DangerousObject. Multi.Generic, seguido por hacktool.Msil. KMSAuto.di con un 9.23%. Mientras que en España los virus que han infectado son el Trojan.winLNK.Agent.gen con el 13.64% y le sigue el HackTool. MSIL.KMSAuto.di con el 8.01%.

PORCENTAJE DE INFECCIONES DE ESPAÑA EN EL ÚLTIMO MES	
NOMBRE	Porcentaje
1.DangerousObject.Multi.Generic	11.4%
2.Hacktool. MSIL.KMSAuto.di	9.23%
3. Hacktool. MSIL.KMSAuto.dh	8.64%
4. Troja.Multi.Agent.gen	7.45%
5. Hoax.Win32.Agent.gen	&.49%
6. Trojan.Script.Generic	3.35%
7. Trojan-Dropper.Android02.Necro.n	3.19%
8.Hacktool. MSIL.KMSAuto.by	2.99%
9.Hacktool. MSIL.KMSAuto.bx	2.96%
10. Hacktool.Win32.KMSAuto.m	2.83%

Ilustración 9 : Porcentaje de Infecciones de España en el último mes. (Kaspersky)[67]

[67] Kaspersky (2019), *Estadísticas de Ecuador mensual de alerta de infecciones.* Recurso Online, disponible en « ttps://cybermap.kaspersky.com/es/stats/#country=35&type=oas&period=w» (última consulta 07 de septiembre de 2019).

PORCENTAJE DE INFECCIONES DE ECUADOR EN EL ÚLTIMO MES	
NOMBRE	Porcentaje
1. Trojan.WinLNK.Agent.gen	13.64%
2.Hacktool. MSIL.KMSAuto.di	8.01%
3 DangerousObject.Multi.Generic	7.83%
4. Hacktool. MSIL.KMSAuto.dh	7.55%
5. Hacktool. win32.KMSAuto.ew	4.94%
6. Hacktool. MSIL.KMSAuto.bx	4.34%
7. Hacktool. MSIL.KMSAuto.by	4.27%
8. Worm.Win32.Autoit.aky	4.26%
9. Hacktool.win32.KMSAuto.m	4.1%
10. Trojan.WinLNK.Starter.gen	3.66%

Ilustración 10: Porcentaje de Infecciones de Ecuador en el último mes (Kaspersky)[68]

En referencia a España el "Centro Nacional de Inteligencia (CNI) detectó el año pasado 38.000 incidentes de ciberseguridad, lo que representa un crecimiento del 43% respecto a 2017." y el Centro de Cristológico Nacional solo en el mes de enero de 2019 a detectado 4000 accidentes [69].

Así también este año ha sido un año extraordinario para el Ecuador en relación con los ciberataques puesto que desde el retiro del asilo a Julián Assange se han recibido más de 40 millones de ciberataques, así Ecuador paso del puesto 51 al 31 en los ciberataques a nivel mundial. Pero, aunque en una menor cantidad antes esto Ecuador ya había sufrido ciberataques bancarios que representaron una perdida para el Banco del Austro de 6 millones de dólares en el año 2016.

Ahora también tenemos marcos de análisis de riesgos de la ciberseguridad como ISO27001, que esta norma se emitió a nivel internacional y determina la seguridad de una empresa y en especial para la seguridad de la información o a su vez como el proyecto H2020 CYBECO Supporting Cyberinsurance from a Behaivoural Choice Perspective que también simulan riesgos aleatorios, como la infección de virus, ciberdelincuencia etc.

[68] Kaspersky (2019), *Estadísticas de Ecuador mensual de alerta de infecciones.* Recurso Online, disponible en « ttps://cybermap.kaspersky.com/es/stats/#country=35&type=oas&period=w» (última consulta 07 de septiembre de 2019)

[69] Abellán, L. (2019). *España recibió un centenar de ciberataques críticos en 2018*. Recurso Online, disponible en « https://elpais.com/politica/2019/02/14/actualidad/1550170544_939859.html» (última consulta 01 de septiembre de 2019)

En base a estos análisis muestran el riesgo que tienen las instituciones bancarias de ser victimas a ataques bancarios y sin duda son elevadas los índices reales diarios. La gran preocupación de estas entidades ha hecho que existan una variedad de seguros que protegen a las entidades ante los problemas de ciber ataques.

Así el primer banco de España que ha contratado estos seguros es el Santander, esta contratación se la ha hecho por dos tipos de cobertura una a nivel local y otra global, este tipo de seguro es considerado como un riesgo del negocio clave. A esto se han sumado también bancos como CaixaBank, Bankia estas dos ultimas tienen contratos con AIG Europe S.A. de Estados Unidos, que su precio medio es de 500.000 euros para la cobertura de 50.000 millones de euros.

Este tipo de seguros tiene cibercobertura sobre los cibercrimenes, vulneración de datos, sanciones, fallos judiciales, interrupción de sistemas, daños de equipos, hasta el daño de imagen y de la reputación de la entidad bancaria. Y en la actualidad existen un sin numero de empresas de seguros que brindar mayores coberturas ante estos eventos. Y ya no solo como un servicio a nivel bancario sino también a empresas y pequeños usuarios.

CONCLUSIONES

Para finalizar la presente investigación podemos sintetizar en que la responsabilidad civil bancaria es una responsabilidad profesional y está basada en la especificación sobre el giro del negocio y las actividades que tiene la entidad financiera. Y aunque esta responsabilidad en un inicio contractual, también se extiende a un sentido extracontractual en especial a lo relacionado con los servicios bancarios.

Evidentemente, los servicios bancarios por medio de la tecnología como la banca online y banca móvil ahora son parte del giro del negocio del banco, ya no solo como un elemento innovador sino como parte fundamental del funcionamiento de estos, por esta razón han tenido que establecer las responsabilidades y obligaciones de estos servicios en contratos específicos. Así también, los entes reguladores han tenido que establecer nuevas normativas y regular los contratos marco de los servicios online.

Otro elemento importante es que la seguridad online ha pasado a tener un rol esencial para las economías mundiales y de los sistemas financieros, ya que un solo error podría causar perdidas millonarias por esta razón los bancos han optado por contratar sistemas como el certificado de seguridad y mecanismos de cifrado de datos que dan una protección adicional a los usuarios. Además de agentes externos que brindas protección a los bancos como empresas destinadas a prevenir ataques bancarios.

A pesar de todos los esfuerzos de la banca para protegerse y tener sistemas más seguros, los cibercrímenes y las vulneraciones a sus sistemas se presentan a cada segundo y aunque las legislaciones de España y Ecuador en sus ordenamientos jurídicos establecen penas por estos, es sin duda el mayor reto encontrar a los responsables ya que estos pueden ser cometidos desde cualquier parte del mundo. Y los usuarios bancarios no cuentan con la información ni conocimiento suficiente para a

Asimismo, hemos realizado una conceptualización de algunos de los cibercrimenes como el Phishing, Ciberestafa, Craking, Vishing, Fake Apps, Malware y todos sus derivados, mostrando que cada día nacen nuevas formas de cometer delitos en el ciber espacio y que algunos de estos conceptos son ignorados por los usuarios bancarios. Y que a pesar que nos encontramos en un mundo que utilizamos a diario la tecnología no estamos conscientes de los riesgos a los que nos exponemos.

En este sentido, podríamos decir que la responsabilidad es compartida por un lado el banco por su giro de negocio debe brindar sistemas de seguridad y por otra en la forma que el usuario bancario gestiona sus datos, equipos electrónicos, claves. Por esta razón en los contratos bancarios se establecen derechos y obligaciones de las partes, pero como lo habíamos mencionado si esta protección parece titánica para sistemas modernos que utilizan los bancos, entonces solamente le queda al banco dar consejos y recomendaciones a sus clientes.

Dentro del análisis expuesto, es posible observar a breves rasgos las protecciones y desarrollos tecnológicos que tienen tanto los bancos españoles como ecuatorianos y la conclusión de esto es que tanto en la práctica social de España como su normativa, ha establecido completamente la gestión bancaria por medio de canales digitales, mientras que en el sistema bancario ecuatoriano aun la gestión sigue siendo en su gran mayoría con el uso del papel moneda y en las agencias físicas. Por esta razón el sistema de protección en sus canales digitales de los bancos ecuatorianos no se compara con los que utiliza la banca española.

De esta forma, la responsabilidad que tienen los bancos en los servicios electrónicos de carácter bancario se le otorga casi por completo al banco, dándole protección al usuario. Tanto la normativa como la jurisprudencia confirman esta posición y, a pesar que el banco haya cumplido con los requisitos de seguridad que le corresponden, esta no es una exoneración de la responsabilidad por el servicio de carácter profesional que esta a su cargo.

BIBLIOGRAFÍA

LEYES

Españolas

- Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio.
- Real Decreto de 24 de Julio de 1889 por el que se publica el Código Civil.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ecuatorianas

- Registro Oficial N.189, de 10 de febrero de 2014. Código Orgánico penal del Ecuador.
- Registro Oficial Suplemento N.46, de 24-jun-2015. Codificación del Código Civil del Ecuador.

FUENTES DOCTRINALES

- Antón, J.(1949). *Derecho Penal.* Madrid : Camargo Hernández.
- Chishti,S, Janos,B. (2017). El Futuro es Fintech. Reino Unido: Jonh Wiley & Son Ltd, pág. 33.
- Cordobera, L. (1993). *Los Daños Colectivos y la Reparación.* Buenos Aires: Editorial Universidad
- Estevil, L. (1989). *Hacia un concepto actual de responsabilidad civil.* Barcelona: Boch. Pág.68
- Gárdo, A. (2016). *Manual de Derecho de Obligaciones.* Valencia: Dykinson. pág. 83

- Martínez, G. (1998). *Responsabilidad Civil Extracontractual en Colombia.* Medellín: Temis.

- Quintano, A. (1963). *Curso de Derecho Penal*. Madrid.

- Real Academia Española. (1999). *Diccionario de la Lengua española.* Madrid: España Calpe.

- Rodríguez, G. (2014). *Responsabilidad Contractual.* Chile : Jurídica de Chile.

- Romero, C. (2008). *Poder Informatico y Seguridad Júridica*. Madrid:Fundesco.

- Rosal, J. (1959). *Lecciones del Derecho Penal Español.* Madrid: S Aguirre Impresor.

- Santiago, C. (2015). *La responsabilidad civil extracontractual de los empresarios.* Madrid: Dyskinson.

- Sarrión, A. (1992). *La Evolución del Derecho de años.* Barcelona: Ponencias y coloquios en la Jornada de Derecho de Daños.

- Tamayo, J. (2007). *Tratado de Responsabilidad Civil*. Ed. II. Bogotá: Legis.

- Velázquez, J. (1996). *El Estudio de caso en las relaciones juridicas internacionales.* Ciudad de Mexico: UNAM.

- Yáguez, R. (1993). *Tratado de Responsabilidad Civil*. Navarra: Revista Jurídica Navarra.

- Yágüez, R. (2008). *La Responsabilidad Civil. Cuestiones Previas de delimitación.* Barcelona: Bosh.

DOCUMENTOS ONLINE

- Abellán, L. (2019). *España recibió un centenar de ciberataques críticos en 2018*. Recurso Online, disponible en « https://elpais.com/politica/2019/02/14/actualidad/1550170544_939859.html» (última consulta 01 de septiembre de 2019)

- ABC Madrid (2001). *Nueva ciberestafa millonaria que afecta a más de 300 personas en España.* Recurso Online, disponible en: « https://www.abc.es/espana/madrid/abci-detienen-24-personas-ciberestafa-millonaria-mas-300-afectados-201907121217_noticia.html» (última consulta: 20 de agosto de 2019).

- AndaluciaCERT. (2017). *Centro de Seguridad*, Recurso Online, disponible en «https://www.seguridad.andaluciaesdigital.es/documents/» (última consulta: 21 de agosto de 2019)

- Bankia Blog (2018). *La ciberseguridad.* Recurso Online, disponible en «https://www.blogbankia.es/es/blog/ciberseguridad-sector-bancario.html» (última consulta: 14 de agosto de 2019)

- Bankia Blog (2018). *La ciberseguridad, el gran reto del sector bancario* . Recurso Online, disponible en «https://www.blogbankia.es/es/blog/ciberseguridad-sector-bancario.html» última consulta: 14 de agosto de 2019)

- BBC News Mundo. (2019). *Por qué la tecnología 5G hará más fácil perseguir a los criminales*, Recurso Online, disponible en «https://www.bbc.com/mundo/noticias-49064315» (última consulta) 22 de julio de 2019)

- BBVA. (2019). *Seguridad*. Recurso Online, disponible en «https://www.bbva.es/sistema/meta/seguridad/index.jsp» (última consulta 30 de agosto de 2019).

- Brunat. D. (2015). *El Ciber-Robo del Siglo.* Recurso Online, disponible en: « https://www.elconfidencial.com/mundo/2015-02-17/el-ciber-robo-del-siglo-sacan-mil-millones-de-dolares-de-varios-bancos-con-un-troyano_713592/ » (última consulta: 13 de agosto de 2019).

- Caixabank (2019). *Aspectos importantes de seguridad Aspectos legales*. *CaixaBank.* Recurso Online, disponible en «https://www.caixabank.es/particular/seguridad/seguridadlacaixa_es.html#garantias_técnicas» (última consulta 30 de agosto de 2019).

- El Comercio (2018). ¿Cuál es la diferencia entre un hacker y un cracker? Recurso Online, disponible en: « https://elcomercio.pe/tecnologia/actualidad/diferencia-hacker-cracker-noticia-490674 » (última consulta: 24 de agosto de 2019).

- El Mundo (2019). *Detenido Lupin, el leonés de 23 años considerado el mayor ciberestafador de la Historia*. Recurso Online, disponble en: «https://www.elmundo.es/espana/2019/07/05/5d1e4d6f21efa0ce7e8b4672.html» (última consulta: 20 de agosto de 2019).

- El Universo, (2018). *Tres de cada diez personas cuentan con smartphone en Ecuador*. Recurso Online, disponible en « https://www.eluniverso.com/noticias/2018/08/06/nota/6893255/tres-cada-diez-personas-cuentan-smartphone» (última consulta 01 de septiembre de 2019).

- Expansión. (2017) (10 de julio de 2017). *Cada incidente de seguridad online supone para la banca una factura media de 1,6 millones de euros.* Recurso Online, disponible en«https://www.expansion.com/economiadigital/companias/2017/07/23/596ca65d22601dbe118b456b.html» (última consulta: 14 de agosto de 2019).

- González, G (2014). *Blogthinkbig.* Recurso Online, disponible en «https://blogthinkbig.com/que-es-el-cifrado» (última consulta: 20 de agosto de 2019)

- Observatorio Español de Delitos Informáticos. (2019). *Reporte de Ciberdelito en España.* Recurso Online, disponible en «http://oedi.es/estadisticas/». (última consulta 3 de agosto de 2019).

- OEA, (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.* Canadá. Recurso Online, disponible en « https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf» (última consulta 01 de septiembre de 2019).

- Panda Security. (2018). «Guía de supervivencia contra ciberatracos millonarios» Recurso Online, disponible en «https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/06/Privacidad-Instituciones-Financieras.pdf.» (última consulta: 14 de agosto de 2019).

- Pibank. (2019). *¿Que es y como funciona el código OTP?* (2019). Recurso Online, disponible en «https://www.pibank.es/faq/que-es-y-como-funciona-cogido-otp/ »(última consulta 30 de agosto de 2019).

- Santander. (2019). *Nuestro Compromiso con tu Seguridad*. Recurso Online, disponible en «Santandehttps://www.bancosantander.es/es/particulares/banca-online/seguridad-online/nuestro-compromiso-de-seguridad». (última consulta 30 de agosto de 2019).

- Santander. (2019). *Que es Trustter Rapport.* Recurso Online, disponible en «https://www.bancosantander.es/es/particulares/banca-online/seguridad-online/ibm-trusteer-rapport.» (última consulta 30 de agosto de 2019).

- Santander. (2019). *Seguridad del Sistema.* Recurso Online, disponible en«https://www.pb-santander.com/es/confidencialidad/seguridad-del-sistema» (última consulta 30 de agosto de 2019).

- Semple.C. (2019). *Los resultados de la transformación digital de BBVA,* Recurso Oline, disponible en « https://www.bbva.com/es/bbvas-digital-transformation-delivering-the-results/» (última consulta) 21 de julio de 2019)

- Unocero. (2017). *Los malware más peligroso y devastadores en toda la historia*. Recurso Online, disponible en «https://www.unocero.com/noticias/los-malware-mas-peligrosos-y-devastadores-en-toda-la-historia/». (última consulta 30 de agosto de 2019).

DOCUMENTOS DE ILUSTRACIONES

- Banco del Pichincha (2019). *Foto Scream de Pantalla de Certificado Electrónico*. Recurso Online, disponible en «wwww.bancodelpichincha.con» (última consulta 19 de agosto de 2019).

- Banco Santander (2019). *Foto Scream de Pantalla de Certificado Electrónico*. Recurso Online, disponible en «wwww.bancosantander.es» (última consulta 19 de agosto de 2019).

- CaixaBank (2019). *Enunciado de aceptación de cookies CaixaBank,cai* Recurso Online, disponible en « https://www.caixabank.es/particular/home/particulares_es.html » (última consulta 30 de agosto de 2019).

- Espinal. J (2018). *Ejemplo de aplicaciones falsas*. Recurso Online, disponible en « https://www.downloadsource.es/como-identificar-app-falsas-o-fraudulentas-en-google-play-para-android/n/11736/» (última consulta 30 de agosto de 2019).

- Kaspersky (2019). *Mapa en tiempo real de amenazas Cibertnéticas.*. Recurso Online, disponible en « https://cybermap.kaspersky.com/es» (última consulta 01 de septiembre de 2019).

- Kaspersky (2019). *Estadísticas de Ecuador mensual de alerta de infecciones.* Recurso Online, disponible en « https://cybermap.kaspersky.com/es/stats/» (última consulta 07 de septiembre de 2019).

- Kapersky (2019). *Estadísticas de Ecuador mensual de alerta de infecciones.* Recurso Online, disponible en « ttps://cybermap.kaspersky.com/es/stats/#country=35&type=oas&period=w» (última consulta 07 de septiembre de 2019).

- Oficina de Seguridad del Internauta (2019). *Ejemplo de Phishing Banco Santander.* Recurso Online, disponible en « https://www.osi.es/es/actualidad/avisos/2018/02/phishing-al-banco-santander » (última consulta 25 de agosto de 2019).